U.S. Nuclear Regulatory Commission
Office of Nuclear Reactor Regulation

NRR OFFICE INSTRUCTION

Change Notice

Office Instruction No.:	**ADM-301, Revision 4**
Office Instruction Title:	**Information Technology (IT) Management**
Effective Date:	**September 28, 2006**
Primary Contacts:	**Michael MacWilliams** **301-415-1877** **mlm4@nrc.gov**
Responsible Organization:	**NRR/PMAS**

Summary of Changes: This issuance of ADM-301, Revision 4, "Information Technology (IT) Management," adds Enclosure 8, which describes the rules of behavior for Automated Information Systems and addresses the Certification and Accreditation requirements for major and listed systems.

Training:	None
ADAMS Accession No.:	ML062420175

U.S. Nuclear Regulatory Commission
Office of Nuclear Reactor Regulation

NRR OFFICE INSTRUCTION

Change Notice

Office Instruction No.:	**ADM-301, Revision 4**
Office Instruction Title:	**Information Technology (IT) Management**
Effective Date:	**September 28, 2006**
Primary Contacts:	**Michael MacWilliams** **301-415-1877** **mlm4@nrc.gov**
Responsible Organization:	**NRR/PMAS**

Summary of Changes: This issuance of ADM-301, Revision 4, "Information Technology (IT) Management," adds Enclosure 8 which describes the rules of behavior for Automated Information Systems and addresses the Certification and Accreditation requirements for major and listed systems.

Training:	None
ADAMS Accession No.:	ML062420175

Position	PIMB:PMAS:NRR	PIMB:PMAS:NRR	PIMB:PMAS:NRR	C:PIMB:PMAS:NRR	D:PMAS:NRR
Name	MMacWilliams	VTharpe	BUsilton	AMendiola	JDavis
Date	08/10/06	08/30/06	08/10/06	09/19/06	09/28/06

OFFICIAL RECORD COPY

NRR OFFICE INSTRUCTION
ADM-301, Revision 4

Information Technology (IT) Management

---

1. POLICY

It is the policy of NRR to have clearly defined guidance for Information Technology (IT) Management.

2. OBJECTIVES

To define and explain the NRR guidance related to IT matters.

3. BACKGROUND

The NRC Office of Information Services (OIS) has overall responsibility for IT policy and procedures. This instruction defines the NRR implementation of OIS instructions and IT-related management directives. The OIS and the Customer Support Center (CSC) have information on the internal web which provides information on the services and support they provide. OIS provides NRC wide guidance on matters such as rules for using shared Local Area Network (LAN) drives, responding to system failures, and dealing with suspect e-mails and viruses. Nothing in this Office Instruction should change or modify the guidance provided by OIS.

NRR has developed an IT Support Web site to facilitate the implementation of IT policy in NRR. The Web site is located at Intranet/NRC Organization/NRR/NRR IT Support. There is also a NRR IT Coordinator Handbook which can be found in ADAMS at ML033350426. This OI identifies which services that Information Management Branch (PIMB) and the NRR IT Coordinator are responsible for and capable of delivering, which services the Division IT Coordinators are responsible for and capable of delivering, and which services that OIS, the Office of Administration (ADM), or others provide, which PIMB and the IT Coordinators simply serve as communicators.

Any questions concerning any of the items listed in this Office Instruction should be directed to the Branch Chief, PMAS/PIMB.

4. BASIC REQUIREMENTS

- **NRR IT Coordinator**

  A member of the PMAS staff will be assigned the role of NRR IT Coordinator. At least one appropriate back-up NRR IT Coordinator will also be designated within PMAS. The duties of the NRR IT Coordinator are defined in Enclosure 1.

- **Division IT Coordinator**

  A member of each division will be assigned the role of Division IT Coordinator. The duties of the Division IT Coordinator are defined in Enclosure 2. Divisions may split up the duties among additional staff members, but one staff member must have the central role. Divisions are encouraged to designate at least one back-up Division IT Coordinator. The Division staff should contact their Division IT Coordinator if they have any questions related to IT.

- **Developing and implementing new computer systems for NRR**

  PIMB must be contacted before any new computer systems are developed or implemented in or for NRR. Specific guidance for the development of new computer systems is contained on the OIS internal Web homepage (CPIC Instructions) and in IT-related Management Directives.

- **Major modifications to existing NRR computer systems**

  Major modifications to existing systems are covered by the same guidance as the development of new systems.

- **Software capitalization**

  All new systems and major modifications to existing applications are covered by special capitalization requirements of the Office of the Chief Financial Officer (OCFO). Both funds and NRC Full Time Equivalents (FTE) are reported to the OCFO for new systems and major modifications to existing applications. NRC FTE is reported using a Technical Assignment Control (TAC) number to capture the FTE expended. PIMB will provide guidance for software capitalization.

- **Management, control, and reporting of IT funds within NRR**

  Budgeting of IT funds is part of the annual budget process. In addition to the "Green Book" and "Blue Book" reporting to Congress, PMAS also prepares an additional attachment that breaks down IT funds and FTE including computer security costs. Division IT Coordinators supply the needed information to PMAS for preparation of this attachment. PMAS also prepares OMB Exhibit 300 for the Reactor Program System (RPS) each year.

  All divisional expenditures of IT funds for equipment and systems development must be approved by PMAS.

- **Installation, relocation, and maintenance of software/hardware**

  For IT equipment, software installation, or relocation, the staff member can submit a request at the NRR IT Support internal Web site. PIMB will review, approve and forward requests to OIS.

- **Disposition scheduling and retirement of computer application systems**

  A "Records Disposition Schedule" must be prepared for each NRR-sponsored computer application that is a primary or secondary records system as defined by the National Archives and Records Administration (NARA). These schedules must be approved by the OIS and/or NARA. If the NRR-sponsored computer application is not a records system (OIS must agree), the computer application can be retired without a NARA-approved schedule. PIMB will provide guidance for developing disposition schedules.

- **Computer Security**

  All Major Applications and "listed" NRR-sponsored computer systems must be reviewed annually to determine whether security plans and certifications are up to date or required to meet the requirements of the Federal Information Security Management Act (FISMA). Security plans for major applications and listed systems must be updated at least every 3 years or when the computer application is significantly modified, whichever is sooner. All computers that process safeguards or classified data must have a security plan.

  There is an annual requirement for all NRR staff to complete the on-line Computer Security Awareness Course.

  The system sponsor shall appoint an Information System Security Officer (ISSO) for each Automated Information System (AIS) for which he or she is responsible. The ISSO position is a trusted position with special access to and authority for an AIS. Thus, ISSO responsibilities should not be assigned to an individual who has other trusted responsibilities (e.g., a System Administrator should not be assigned ISSO responsibilities).

  All systems should check input for accuracy, completeness and validity and identify and handle error conditions in an expeditious manner.

  All users of NRR Automated Information Systems shall follow the Rules of Behavior provided in Enclosure 8.

- **Computer system inventory**

  OIS maintains a list of agency computer applications. PIMB is responsible for maintaining the information on NRR-sponsored computer systems. Each active NRR sponsored computer system must have an NRR contact. This includes new systems that are under development or systems that are in the process of being retired.

- **Personal Digital Assistants (PDAs)**

  At the present time, PDAs are considered only for staff who have frequent travel requirements, are participants of an IT initiative, and/or have specific programmatic needs. In addition, funds would have to be available and specific

approvals would have to be provided through the management chain (currently the Director, PMAS, has final approval).

- **Ergonomics**

  Workstations that require significant modifications, and requests for chairs, are submitted to the Office of Administration (ADM) for processing. Requests should be submitted on an NRC Form 30 and submitted to the Ergonomics Coordinator in PMAS/PIMB for review, signatures, and forwarding to ADM. Minor ergonomic type IT requests (mouse, trackball, etc.) may be submitted to the IT Support Website as a "Purchase Request." Otherwise, the formal workstation analysis report should be provided to PIMB. See Yellow Announcement 02-0054 dated July 23, 2002 (ADAMS Accession No. ML022040566) for more detail and guidance on the "Workstation Ergonomic Program."

- **Flexiplace (Telecommuting)**

  Laptops acquired for the divisions are loaded by the Customer Support Center (CSC) with CITRIX, WordPerfect Suite (from OIS) and Microsoft Office XP Pro Suite (from NRR). These laptops are available for Flexiplace use at the divisions' discretion.

  OIS has authorized NRR to acquire and provide software (at NRR expense) for home use to staff members where appropriate. Staff members can load the software on their own home computers themselves. OIS already provides CITRIX and the WordPerfect Suite for this purpose.

  NRR will not provide unique software for home use that has the effect of reproducing an employee's NRC workstation. Individuals, however, can apply for software and have it considered on a case-by-case basis.

  Anyone who is granted authorization and receives software for home installation and use must sign an NRR-provided acknowledgment and waiver form that states, among other things, that the user installs the software at their own risk and must return the software upon completion of the project or departure from NRR. PMAS staff keeps the signed acknowledgment forms on file. A copy of the agreement is provided in Enclosure 3.

- **Cell Phones/Pagers**

  PIMB will provide cell phones, accessories, and service to the Executive Team members, Leadership Team members, the Director's Technical Assistant, the Day Emergency Officer, and the Night Emergency Officer. Acquisition and use of any other cell phones or pagers (provided by OIS) may be submitted to OIS via the NRR IT Support internal Web site using a "Miscellaneous Request". A copy of the NRR cell phone service agreement is provided in Enclosure 4.

- **Foreign Assignees**

Foreign Assignees to NRR will be provided a standalone workstation and desktop printer (supplied by the NRR Office IT Coordinator or OIP) with no connectivity to the NRC LAN/WAN. In addition, foreign assignees will not be permitted access to agency standard applications, ADAMS, or HRMS.

- **NRR Color LAN Printer Usage**

  In coordination with OIS, NRR's Information Management Branch will provide color LAN printer capability to each division and each floor in space occupied by the office.

  Color laser printers have more working parts and smaller toner cartridges than the standard black-and-white LAN printers. In addition, color cartridges cost more. As such, the printers require more personal attention and greater care. In order to maintain these printers at their best operating levels for the longest periods of time, the NRR divisions and staff shall assume the following responsibilities:

  Staff shall not use the color printers to make transparencies. If transparencies are needed, a clean color original on white paper shall be made and transparencies requested from the reproduction center (P1 level).

  An "owner" of each printer shall be appointed from each division who will monitor the printer(s) to address the need for supplies and maintenance.

  Staff shall not use the color printers as substitutes for black-and-white printers. All black-and-white print jobs shall be sent to the black-and-white printers, even if they are less conveniently located.

  Staff shall use color as an effective communications tool, not "just because it is available." If a document is appropriate in black-and-white, black-and-white shall be used.

  Staff shall not use the color printers as color copiers. Copies are to be requested from the reproduction center. (In addition, color backgrounds for slides should be avoided, if possible.)

- **Security Verification Process for Access to the NRC LAN/WAN**

  Access to the NRC LAN/WAN is provided only to those who need access for the performance of their duties and meet the security requirements. A user ID and associated password are required to access the LAN/WAN. NRR requests for a user ID must be submitted to the CSC by the NRR Office IT Coordinator via the NRR IT Support internal Web site.

  For *NRC employees* requiring access to the LAN, the NRR Office IT Coordinator must verify that NRC employee for whom they request a user ID have been granted a "Q" or "L" security clearance, or a 145b waiver. For *NRC contractors*, the NRR Office IT Coordinator must contact the NRR Security Officer (or NRR Project Officer that the contractor employee is working under) to verify the contractor has been issued either

a "Q" or "L" security clearance, or an IT Level I or II access. For additional information regarding the security verification process, please refer to the OIS memorandum on "Security Verification Process for access to the NRC LAN/WAN" dated May 27, 2003 (ADAMS Accession No. ML031290053).

- **ADAMS Access for NRR Contractors and Consultants**

  A memorandum from the Division Director, PMAS, is required to obtain an ADAMS user account and password for NRR contractor staff only. Both contractors and consultants are required to sign and submit the ADAMS Non-Disclosure Statement for access to ADAMS documents. The ADAMS Non-Disclosure Statement can be downloaded from ADAMS (Accession No. ML022630226). The original signed form is retained by the Contract Project/Task Order Manager and a copy sent to OIS, T-5F-11, for processing.

- **Use of Personally-Owned Equipment**

  NRC staff may contact the CSC for assistance with problems encountered using CITRIX with their personally-owned equipment. The CSC will attempt to help the user determine if the problem is with the modem or address other issues that can be resolved over the telephone such as checking software settings.

  [NOTE: Modems that are CITRIX-approved can be located on the CSB website: (http://csb.nrc.gov/upload/reference/modem.asp **]**

- **Purchasing IT hardware and/or software not supplied by OIS as part of the basic NRC infrastructure**

  PMAS budgets for procurement of IT hardware and/or software not supplied by OIS as part of the basic NRC infrastructure. If a division anticipates an unusually high level of procurement activity for expensive items such as laptops, PMAS should be notified during the budget process or the division should request separate funding. IT hardware and/or software not supplied by OIS as part of the basic NRC infrastructure is defined in Enclosure 5.

- **Requests for all other IT-related services or actions**

  For all other IT-related services or actions, such as additional network memory or inclusion in an e-mail distribution group, the staff member submits a request at the NRR IT Support internal Web site using a Miscellaneous request. A sample of the services provided at the Web site is provided in Enclosure 6.

  The Property Management requirements for IT equipment can be found in NRR Office Instruction ADM-202 "NRR Policy on Property Management."

  OIS contractors do not provide hands-on service for personally-owned devices. Refer to Management Directive 2.7, "Personal Use of Information Technology," regarding the use of IT resources (including IT contractor services) for personal use.

The CSC staff will take calls for personally-owned devices such as PDAs that are attached to NRC equipment. In the case of PDAs attached to NRC on-site desktops, a technician may be dispatched to determine if the problem is with the PC or NRC-provided software. The technicians will not perform service on personally-owned equipment. **[NOTE**: Neither the NRC nor its contractors will assume any liability for loss or damage to non-NRC owned equipment.**]**

- **Reactor Program System (RPS)**

  RPS is a work planning and staff resource management system that provides NRR and the Regional staff power reactor inspection and work planning, scheduling, and reporting capabilities. RPS is used by NRR and the Regions to plan and schedule work assignments and inspection activities. The assignments and schedules entered into RPS are passed electronically to the Human Resources Management System (HRMS) where Time and Labor (T&L) data is collected. The official record copy of T&L data is maintained in HRMS. When daily T&L hours are retrieved from HRMS, they are edited and rolled up into one record per week per individual. The NRR and the Regions T&L data is stored in the RPS database. The RPS database also includes inspection information, plant performance indicators, inspection follow-up items, NRC staff data, facility characteristics, and other reactor regulatory data. The data in RPS is one of the tools used by NRC managers to assess the effectiveness and uniformity of the implementation of the NRC reactor inspection programs. Additional RPS requirements are listed in Enclosure 7.

5. RESPONSIBILITIES AND AUTHORITIES

The responsibilities of the Office Director and NRR staff related to IT are detailed in the Management Directives listed in Section 10. All NRR staff are required to follow guidance contained in NRC Management Directives and NRC documents listed in Section 10. These documents incorporate requirements from applicable laws and regulations and guidance from OMB, NARA, NIST, and other agencies. Division IT Coordinators and PMAS staff can provide assistance in this area.

6. PERFORMANCE MEASURES

No performance measures for this Office Instruction have been developed at this time.

7. PRIMARY CONTACT

Michael L. MacWilliams
NRR/PMAS/PIMB
301-415-1877
mlm4@nrc.gov

8. RESPONSIBLE ORGANIZATION

NRR/PMAS/PIMB

9. EFFECTIVE DATE

September , 2006

10. REFERENCES

The applicable laws or regulations affecting IT include statutory requirements, National Institute of Standards and Technology Special Publications (NIST SP), Federal Information Processing Standards Publications (FIPS PUBS), OMB bulletins and budget circulars, NRC publications, and U.S. Department of Commerce (DOC) publications. The PMAS or OIS staff can assist in finding the applicable, current references. The OIS internal Web site contains links to many references and contains the latest versions of the NRC references.

Partial listing of references:

- Computer Fraud and Abuse Act of 1986, as amended, Public Law 99-474 (18 United States Code [U.S.C.] 1001 note).
- Computer Security Act of 1987, Public Law 100-235 (40 U.S.C. 739 note).
- The Freedom of Information Act, 5 U.S.C. §552, As Amended by Public Law 104-231, 110 Statute 3048, March 31, 1997, which includes the Electronic Freedom of Information Act Amendments of 1996.
- Paperwork Reduction Act, Public Law 96-511, 1980.
- Privacy Act of 1974, Public Law 93-579.
- U.S. Department of Commerce Abbreviated Certification Methodology Guidelines for Sensitive and Classified Information Technology Systems, December 1992.
- Federal Information Security Management Act (FISMA).
- Americans with Disabilities Act (ADA).
- U.S. Nuclear Regulatory Commission (can be found on OIS internal web page):
  - NRC Management Directive 2.1 Information Technology Architecture.
  - NRC Management Directive 2.2 Capital Planning and Investment Control.
  - NRC Management Directive 2.3 Telecommunications.
  - NRC Management Directive 2.6 Information Technology Infrastructure.
  - NRC Management Directive 2.7 Personal Use of Information Technology.
  - NRC Management Directive 2.8 Project Management Methodology (PMM) (In draft)
  - NRC Management Directive 12.2 , Classified Information Security Program.
  - NRC Management Directive 12.3, NRC Personnel Security Program.
  - NRC Management Directive 12.4, NRC Telecommunications Systems Security Program.
  - NRC Management Directive 12.5, NRC Automated Information Systems Security Program.
  - NRC Management Directive 12.6, NRC Sensitive Unclassified Information Security Program.
  - NRC Management Directive 13.1, Property Management.
  - NRC Emergency Protection Plan.
  - NRC OIS System Development and Life Cycle Management (SDLCM) Methodology.
- NARA Publication: “Disposition of Federal Records: A Records Management Handbook.”

ADM–301 - Change History			
Date	**Description of Changes**	**Method Used to Announce & Distribute**	**Training**
07/03/2002	This is the initial issuance of ADM-301, "Information Technology (IT) Management." The objective of this office instruction is to define the NRR policy related to IT matters.	E-mail to NRR staff	None
07/16/2004	Rev 1. This is a revision of ADM-301, "Information Technology (IT) Management." Additional IT services provided by NRR are included. The objective of this office instruction is to define NRR policy related to IT matters.	E-mail to NRR staff	None
01/06/2006	Rev 2. This is a revision of ADM-301, "Information Technology (IT) Management." Reference to OCIO changed to OIS. Enclosure 7 added for the Reactor Program system (RPS).	E-mail to NRR staff	None
02/14/2006	Rev. 3. This is a revision of ADM-301, "Information Technology (IT) Management." Text has been added at the end of Attachment 7 which describes how the Regional users are granted access to RPS modules. This change is needed to complete Recommendations 1 and 4 of the IG Audit of the RPS.	E-mail to NRR staff	None
09/28/2006	Rev. 4. This issuance of ADM-301, Revision 4, "Information Technology (IT) Management," adds Enclosure 8, which describes the rules of behavior for Automated Information Systems and addresses the Certification and Accreditation requirements for major and listed systems.	E-mail to NRR staff	None

Enclosures:
- Role of NRR IT Coordinator
- NRR Division IT Coordinator Responsibilities
- Agreement and Rules for Use of NRC-Owned Software on Non-NRC Personal Computer
- Description of NRR Cell Phone Service Agreement
- Procedure for NRR Purchase Card Acquisitions of IT Hardware or Software
- Sample Contents of NRR IT Support Web Site
- Reactor Program System (RPS)
- Rules of Behavior for NRR Automated Information System (AIS) Users

ROLE OF NRR IT COORDINATOR

The NRR IT Coordinator is responsible for coordination of all office IT service requests, procurement of IT hardware and software, reporting changes in Office staff, coordination of agency-wide upgrades, planning/requesting for all IT activities associated with moves, maintaining local IT inventories, and prioritizing and tracking service requests.

FUNCTIONS include:

- Serves as the point of contact for **all** IT service requests for hardware and software, network, telephone, pagers, trouble tickets, moves, procurement, refreshes, upgrades, and office-specific requests.

- Reviews, approves and tracks all IT service requests. This includes ISDN telephone assignment, K-box installation/activations, modems, creating/deleting voice mail accounts, calling cards, hardware/software installations, color printer access, and remote access. Approval by the NRR IT Coordinator is required before submitting the request to OIS.

- Schedules and plans all requests for LAN account changes and/or moves, telephone number moves, equipment moves and upgrades in accordance with OIS guidelines for time requirements. Works with OIS staff to accomplish advance planning guidelines and schedules. Provides move information on electronic move sheet, and identifies non-infrastructure items to be moved.

- Reviews all requests for hardware installation to ensure there is sufficient time and coordination. Forwards requests for processing and scheduling to the CSC.

- Reviews all requests for software installation to ensure there is sufficient time and coordination. Forwards requests for processing and scheduling to the CSC.

- Reviews all requests for service for NRC hardware and software. Responsible for any follow-up client contact when the client is unavailable.

- Ensures that all requests for new PCs or components are properly documented. For new employees, ensures that appropriate staff submit a NEW EMPLOYEE request via the NRR IT Support internal Web site.

- Approves requests for CITRIX Access and Web Access accounts submitted via the NRR IT Support internal Web site.

- Approves requests for new telephone service, K-box installations/activations, and modems are submitted via the NRR IT Support internal Web site.

- Re-prioritizes all open service requests by notification to the OIS CSC when priorities change.

- Notifies OIS regarding all Office changes in organizational staffing structure, and prior to re-organizational changes. Notifies OIS immediately of all IT Coordinator personnel changes.

- Notifies the NRR Office staff of global outages to infrastructure network, Internet services,

hardware and application immediately following official notice by OIS. In addition, notifies Office staff when services have been restored.

- Works with the Property Custodians to maintain records of all IT hardware. Coordinates communication with Property Custodians to report missing items to Security. Identifies items that should be declared as surplus or removed to excess.

- Serves as the liaison between Office staff and OIS in the planning, coordination, and monitoring of agency-wide refreshes, as well as upgrades to hardware and software.

- Attends meetings and briefings with OIS staff on IT issues. Schedules periodic individual meetings with OIS staff to discuss specific office concerns as needed.

- Provides informative and timely feedback to OIS regarding the quality and timeliness of IT services. Makes written (e-mail) recommendations to OIS on ways to improve service and processing of service requests. Notifies OIS staff when IT services are not performed in accordance with required Service Level Standards.

- Procures non-infrastructure hardware and software using the NRC Purchase Card program. All items procured must have OIS authorization prior to purchase.

- Requests additional LAN space for end-users, monitors the space utilization for their specific office, creates/deletes LAN accounts. Requests network configuration changes, includes requests to create network group, requests for access to a specific network group, and requests to move LAN accounts.

- Conducts periodic meetings (at least quarterly) with NRR Division IT Coordinators to provide information related to IT policy, procedures, new software, etc. Instructs new Division IT Coordinators on their duties and responsibilities upon their appointment.

- Ensures that Division IT Coordinators are aware of OIS policies, procedures, and new hardware and software that may increase staff efficiencies/effectiveness.

NRR DIVISION IT COORDINATOR RESPONSIBILITIES

The NRR Division IT Coordinator is responsible for coordination of division IT service requests, approving requests for procurement of IT hardware and software for the division, working with the NRR IT Coordinator on efforts associated with moves, maintaining local IT inventories, and prioritizing and tracking service requests. This includes:

New Employee Submissions

- Coordinating office space assignments with the PMAS/PIMB staff.
- Determining phone needs such as new phone, or voice mail account set up.
- Determining any special network resource mappings that the new employee will require.
- Completing and submitting the "New Employee" questionnaire on the NRR IT Support internal Web site when appropriate.

Equipment Excesses

- Determining the disposition of equipment which is made available through employee moves, retirements, or upgrades.
- Completing and submitting the "Equipment Excess" questionnaire on the NRR IT Support internal Web site.

Employee Moves

- Coordinating staff relocations/office assignments with the PMAS/PIMB space coordinator.
- Determining phone needs such as telephone number move.
- Assisting staff members with move request submissions as needed.
- Completing and submitting the "Employee Move" questionnaire on the NRR IT Support internal Web site for empty office equipment moves, when appropriate.

Division Organizational Change Notifications

- Notifying the NRR Office IT Coordinator of changes in division and/or branch configurations.
- Notifying the NRR Office IT Coordinator of division, branch chief and secretarial changes.

Employee Terminations

- Completing and submitting the "Service Termination" questionnaire on the NRR IT Support internal Web site when signing a termination form for a departing employee (normally, this is an Office IT Coordinator responsibility, but it is passed to Division IT Coordinators on occasion).

Device Refreshes

- Identifying CPU's and/or monitors which are eligible to be refreshed.
- Completing and submitting the "Device Refresh" questionnaire on the NRR IT Support internal Web site when appropriate.

Purchase Approvals

- Logging onto the NRR IT Support internal Web site and approving or rejecting purchase requests submitted by division employees (someone at the branch chief level or higher can approve a purchase request by E-mail to the NRR IT Coordinator if the Division IT Coordinator is absent; in this case, the IT Coordinator would log onto the site and approve or reject the purchase request as directed). The divisions are responsible for ensuring requests are consistent with the division IT needs.

- See Enclosure 3 for more detail concerning IT acquisitions.

Internal Equipment Moves

- Requesting the move of division-specific equipment when necessary to accommodate office maintenance or other activities.

AGREEMENT AND RULES FOR USE OF NRC-OWNED SOFTWARE ON NON-NRC PERSONAL COMPUTERS
(Office of Nuclear Reactor Regulation)

Please read the following statements before signing this agreement. By signing this agreement you acknowledge that you have read and agree to abide by the policies, procedures and rules governing the use of NRC-owned software on non-NRC personal computers and equipment.

1. The NRC-owned software shall be used only for NRC official business.

2. Transfer of classified information to the non-NRC device is strictly prohibited.

3. Transfer of safeguards information to the non-NRC device is strictly prohibited.

4. Transfer of sensitive unclassified data to the non-NRC device is strictly prohibited.

5. The user is responsible for protecting the security and integrity of the NRC information and files contained on non-NRC personal computers and equipment according to Federal law, regulations and NRC policy.

6. The user certifies that installation of any NRC software on non-NRC equipment will not violate licensing agreements. Notwithstanding such certification, any penalties associated with the violation of such licensing agreements are the sole responsibility of the user.

7. Neither the NRC nor its contractors assume any liability for loss or damage to non-NRC equipment, software or data resulting from the use of NRC-owned software on non-NRC personal computers and equipment.

8. Neither the NRC nor its contractors will provide any installation or maintenance services associated with the installation or use of NRC-owned software on non-NRC personal computers and equipment.

9. The software shall be returned in full working order to the NRC at the termination of the project or prior to the termination of employment. Prior to return, the software shall be uninstalled from the non-NRC equipment. The software shall be returned with all original packaging and documentation.

Software provided:_____
_____

Acknowledged:

EMPLOYEE SIGNATURE:_____DATE:_____

PRINTED EMPLOYEE NAME::_____
_____

DESCRIPTION OF NRR CELL PHONE SERVICE AGREEMENT

NRR cell phones are under the Verizon Wireless "America's Choice Business SharePlan."

Currently, 13 lines share 300 "anytime" minutes per month (3,900 minutes total per month available across all lines) at a net cost of $31.05 per line.

Although the plan provides full, nationwide coverage, the base minutes apply only on the Verizon Wireless Network under this price plan, which is roughly two-thirds of the country, mostly excluding the west, Alaska, and Hawaii. (The coverage map is available on the verizonwireless.com web site.)

When your phone's roaming indicator is off or the banner display reads "Verizon Wireless Network," America's Choice 'home' air time rates apply and when the digital indicator is on, digital features and services including national mobile-to-mobile are available.

When the roaming indicator is flashing or the banner reads "Extended Network," America's Choice home air time rates still apply, however, national mobile-to-mobile and some other features and services are not available.

When the roaming indicator is solid or the banner display reads "Roaming," roaming rates apply. National mobile-to-mobile and other services are not available.

Roaming costs $0.69 per minute.

All business calls, roaming or otherwise, will be paid by the NRC.

Rules for personal calls that apply to regular desk phones apply to the cell phones as well, as long as they are within the plan and therefore incur no additional charge to the Government.

Some personal calls under roaming may require reimbursement to the NRC.

Monthly statements which incur no additional charges will not be distributed routinely to the phone holders. They will be made available upon request.

Statements which incur additional charges will be provided to the phone holder for review.

If a reimbursement is required, a check made to "NRC" for the proper amount is to be taken to Leah Tremper (x7347), OCFO/DAF, at T-9 E3, or sent to OCFO/DAF at Mail Stop T-9 E10 with a note that it is for reimbursement of cell phone charges.

PROCEDURE FOR NRR PURCHASE CARD ACQUISITIONS OF INFORMATION TECHNOLOGY HARDWARE OR SOFTWARE

Purchase Card Acquisitions of IT Hardware or Software

NRR Purchase Card acquisitions of Information Technology (IT) hardware or software are accomplished through two mechanisms, depending on the nature of the purchase. First, staff desiring to make an IT hardware or software purchase utilizing PMAS funding for basic items are to go through the NRR IT Support internal web site. Second, staff desiring to make any other type of purchase should complete a Form 30 and take it to the NRR Purchase Card Coordinator.

For basic IT hardware or software, the staff member submits a "Purchase Request" at the NRR IT Support internal web site (Intranet/NRC Organization/NRR/NRR IT Support). This request is automatically forwarded to his or her Division IT Coordinator. If the Division IT Coordinator approves, the database record captures a priority number, the record is entered on an Excel spreadsheet purchase log, and two e-mails are generated for use by NRR purchase agents. One e-mail is then sent to OIS to obtain the required OIS approval. The second e-mail may be used to make the actual purchase order. If the Division IT Coordinator disapproves, the record is removed from the database and the Division IT Coordinator must inform the requestor of the disapproval.

If OIS approves the purchase request, either the second e-mail is forwarded to an appropriate vendor or a vendor is contacted by telephone, fax, letter, or other means. If OIS disapproves the purchase request, the reason is forwarded back to the requestor and the Division IT Coordinator.

NRC Form 30 is to be used for the acquisition of IT hardware or software to be funded out of specific program (non-PMAS) accounts. Normal approval processes for the form must be followed, including receiving certification of funding from NRR/PMAS/PPRB.

All rules associated with the use of the Purchase Card apply, including the single-purchase limit of $2,500.00.

Acquisition of Personal Desktop Printers

The following criteria will be applied regarding the approval by the Division IT Coordinators within the NRR when acquisition of a personal desktop printer is requested:

The request will be approved for -

- Secretaries
- Technical Assistants
- Senior Level Service
- Special Assistants
- Team Leaders
- Section Chiefs and Above
- Staff Performing Sensitive Functions, e.g., allegations, safeguards, personnel, IT coordination, purchase card, budget, classified, security, naval reactors
- Staff Requiring Medical Accommodation, e.g., handicapped, ergonomic assessment
- Foreign Assignees (if not provided by the Office of International Programs)

Special Purposes or Facilities, e.g., task forces inside closed or secure rooms

Requests outside the scope above will not be approved. An appeal may be made to the Director, PMAS.

All staff with existing personal desktop printers will be allowed to keep them. If a replacement machine is subsequently requested, the request is subject to the criteria identified above.

NRC Business Cards

Effective May 29, 2001, the Executive Director for Operations (EDO) determined that, for eligible employees, expending appropriated funds for business cards directly contributes to the NRC mission.

Eligible employees are considered those who perform official representational duties requiring them to interact with outside entities (e.g., licensees, utilities, members of the public, State and local officials, contractors, Federal agency officials, and law firms). NRR employees must receive eligibility approval by their Division Director prior to submitting requests to PMAS/PIMB for business card purchases. **[Note**: Bankcard purchases are only used for large quantities of business cards - 250 or more. Eligible employees who wish to print smaller quantities of business cards in-house may obtain business card paper from their division. Division secretaries may obtain the paper from the NRR FAST team.**]**

For more information on the NRC Business Card Policy, go to the NRC internal Website at the following URL: http://www.internal.nrc.gov/ADM/BUSINESS-CARDS/index.html.

SAMPLE CONTENTS OF NRR IT SUPPORT WEB SITE

The following functions are supported at the NRR IT Support internal web site (Intranet/NRC Organization/NRR/NRR IT Support).

CITRIX Account
Device Refresh
Distribution Group Add
Employee Move
Equipment Excess
GroupWise Resource Add
Hardware Install
Hardware Acquisition
LAN Account Move
LAN Space Upgrade
New Employee
Printer Mapping
Purchase Request
Resource Owner Change
Service Termination
Software Install
Software Transfer

REACTOR PROGRAM SYSTEM (RPS)

The Reactor Program System (RPS) is used by NRR and the Regions to plan and schedule work assignments and inspection activities and record inspection findings. RPS supports the NRC's reactor inspection and licensing programs. It is the responsibility of the RPS users to ensure information in RPS is accurate and timely. The NRC's inspection program is an integral part of the Reactor Oversight Process (ROP) and is important in providing confidence in the continued protection of the public health and safety. Implementation of the ROP is defined in Inspection Manual Chapter 0306, "Information Technology Support for the Reactor Oversight Process." RPS (including the Inspection Planing (IP) and Inspection Reporting (IR) modules) provides a tracking mechanism for the inspection program with respect to scheduling and completion of individual inspection activities, and the data entered is used to verify program completion. The Time, Resources and Inventory Management (TRIM) Module is used by NRR to support the licensing program and other NRR activities. The accuracy of RPS data is paramount in ensuring continued public confidence in the NRC's inspection and licensing processes.

RPS is defined as a Major Application in accordance with NRC Management Directive 12.5, NRC Automated Information Systems Security Program. An OMB Exhibit 300 must be completed each year for RPS. RPS must be certified and accredited every three years or whenever a major modification is made to the system. Access control requirements including purpose, scope, roles, and responsibilities must comply with FIPS-200 and NIST 800-53. NIST SP 800-12 provides additional guidance on security policies and procedures.

User access to client server systems including the RPS modules is monitored and approved by the headquarters office and by each regional office. The RPS Security Access Module (SAM) is used to control access. Each Office/Region will conduct a periodic review of all Office/Region staff with access to client server systems including the RPS modules and will remove access from those who no longer need access. This review will be conducted at least once a year. The access rights of staff who leave the NRC or transfer to a different office are automatically removed by the RPS software.

Each Region will assign an individual to serve as the Regional counterpart. NRR will conduct periodic RPS counterpart meetings. Each Regional Counterpart is responsible for gathering RPS user concerns for their respective region prior to counterpart meetings. In addition NRR will conduct an annual user survey of regional RPS users. Results from this survey will be discussed at the next scheduled Regional counterpart meeting. Counterpart meetings may be conducted via conference call, video teleconferencing, or face-to-face meetings.

Requests for technical support, or enhancements for all RPS modules except TRIM should be sent to the e-mail address RPSHELP. The RPSHELP e-mail address is used by the RPS support team to monitor user feedback. A log is maintained with all RPSHELP e-mails. This log is monitored daily to ensure all incoming e-mails are responded to within two work days. It is the goal of the RPS support team to respond the day the request is received. Requests for TRIM support should be sent to the e-mail address TRIMHELP. TRIM is supported by the NRR Work Planning Center (WPC) staff.

Each Office/Region is responsible for providing RPS training to their users. The Regional Counterparts provides periodic refresher training and classes tailored to different RPS user responsibilities. The NRR RPS support staff will provide training to the Regional Counterparts and will provide training to the regional staff when requested.

Access and privileges to RPS modules:

Upon approval, a user is provided with base level access to an RPS module. Depending on the roles/responsibilities of the user, additional levels of access can be provided. This allows users the capability to enter/update data that is not provided for those with base level access.

IR

General 1 - The user must be provided access to the application in the RPS database. Without this, no user can activate the application.

General 2 - Updates can only be done by the users from the respective regions associated with the Docket(s), with one exception. NSIR can update items associated with their own inspection reports (except Power Reactors).

ROP Sample Size -

Lockout - Users may not modify data after March1st of the year after the end of the associated IP cycle.

Certification - After entering samples, an authorized user may certify entry at the inspection report level. Once certified, data cannot be modified. A small number of users are designated as “super-users" and can de-certify an inspection report. Once de-certified, an authorized user may modify the data. The inspection report is then re-certified.

TI Status -

Certification - After entering TI completion status, an authorized user may certify entry at the TI level. Once certified, data cannot be modified. A small number of users are designated as 'super-users" and can de-certify TI procedures. Once de-certified, an authorized user may modify data. The TI is then re-certified.

IP

General 1 - The user must be provided access to the application in the RPS database. Without this, no user can activate the application.

General 2 - Updates can only be done by the users from the respective regions associated with the Docket(s).

IP is also limited to Operating Power Reactors, Decommissioning Reactors, Fuel, ISFSI, and COLs.

TI Status -

Certification - After entering TI completion status, an authorized user may certify entry at the TI level. Once certified, data cannot be modified. A small number of users are designated as “super-users" and can de-certify TI procedures. Once de-certified, an authorized user may modify data. The TI is then re-certified.

ROP Completion Status tab -

Lockout - Users may not modify data after March1st of the year after the end of the associated IP cycle.

IPAS

General 1 - The user must be provided access to the application in the RPS database. Without this, no user can activate the application.

General 2 - The user must be defined to have update capability for the application. Otherwise, the user has only view access.

General 3 - Separate access definition for the user is needed for the Baseline Procedure process.

IPC

General 1 - The user must be provided access to the application in the RPS database. Without this, no user can activate the application.

General 2 - The user must be defined to have update capability for the application. Otherwise, the user has only view access.

General 3 - Updates are restricted to regional users only. The users can only update IPC's for the dockets in their region.

IRTS

General 1 - The user must be provided access to the application in the RPS database. Without this, no user can activate the application.

General 2 - The user must be defined to have update capability for the application. Otherwise, the user has only view access.

General 3 - Updates are restricted by office. The users can only update inspection reports for their office.

REPORTS

General 1 - The user must be provided access to the application in the RPS database. Without this, no user can activate the application. No data can be entered or updated through Reports.

RULES OF BEHAVIOR FOR NRR AUTOMATED INFORMATION SYSTEM (AIS) USERS

AIS users are any individuals who have been authorized access to or use of an NRC AIS for any reason (e.g., support of an agency mission or developing or maintaining an AIS). Users of an AIS are often the first to encounter an anomaly that may be indicative of an attack or unauthorized actions of a malicious program code. Thus, an AIS user community can serve as a control or countermeasure to identify potential attacks and mitigate the resulting adverse impacts through early recognition, reporting, and compliance with NRC security measures.

Users of an NRC AIS must be authorized before being granted access to an NRC AIS. The assets to which the user is authorized access are to be used in support of NRC mission objectives. These assets may not be used for any non-Government activity, except in accordance with the NRC limited personal use policy (see MD 2.7, "Personal Use of Information Technology").

The NRC user rules of behavior are to be followed by all users of the NRC local-area network/wide-area network (LAN/WAN) system and all users of any NRC AIS. Users shall be held accountable for their actions on the NRC LAN/WAN system. If an employee violates NRC policy regarding the rules of behavior for use of any NRC AIS and the NRC LAN/WAN system, they may be subject to disciplinary action at the discretion of NRC management.

Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, termination, or prosecution under applicable Federal law consistent with the nature and the severity of the violation. The Office of the Inspector General (OIG) is charged with investigation of allegations of misconduct related to misuse of the systems, and all allegations of violations shall be reported to the OIG.

Users shall take appropriate precautions to protect the assets (hardware, software, data) provided for their use or to which they have been granted access (e.g., workstations, microcomputers, local-area networks (LANs), and associated data). An AIS user—

• Shall have no expectation of privacy for information processed by, stored within, or transmitted through the NRC computing environment. Others with access to NRC resources may view such information accidentally or intentionally as they also use, manage, or maintain those resources.

• Shall protect all information and outputs including sensitive unclassified information, classified information or SGI in his or her possession from unauthorized access, disclosure, modification, misuse, damage, or theft.

• Shall not knowingly introduce any malicious code into the computing environment nor attempt to bypass or circumvent security features.

• Shall take appropriate precautions to avoid malicious software when introducing files into the NRC computing environment through physical media (e.g., diskette) or communications (e.g., e-mail attachments, downloading from the Internet).

• Shall not knowingly access or download material (e.g., pornography) that could

create a “hostile work environment.”

• Shall not install any computer program into the NRC computing environment if there is any question that the computer program may not be properly licensed.

• Shall protect all user IDs and associated passwords issued to him or her and will not disclose the password to anyone. Will change his or her password when a possible compromise is suspected and at least every 90 days.

• Shall immediately notify the NRC Customer Support Center of any events that may be perceived to be a potential security incident. The user will also support investigation and resolution of the reported incident. For NRC employees assigned outside of headquarters, the regional office IT staff shall also be contacted.

• Shall attend initial indoctrination and annually complete the computer security awareness refresher training and implement security instructions as directed by NRC security and supervisory personnel.

• Shall comply with all policies and procedures related to the security of NRC LAN/WAN system data and NRC AISs. Classified information and SGI shall not be processed on the agency unclassified LAN. (SGI may be transmitted through the Internet when encrypted and with approval of the transmission procedures and encryption methodology by OIS.)

• Shall report security-relevant events to the OIG and to supervisors, or to the personnel responsible for the security of the NRC LAN/WAN or NRC AISs. These events include security infractions by coworkers, attempted access by unauthorized personnel, violations of procedures, disclosure of sensitive information, loss of availability of NRC LAN/WAN system resources, destruction of data, or detection of erroneous information or unexplained system activity.

• Shall provide immediate notification to supervisory personnel when a decision is made to retire, resign, transfer, or otherwise change the basis for which access to NRC AIS or the NRC LAN/WAN system has been granted.

• Shall select passwords that are at least six characters long, are a combination of both numbers and characters, and cannot be associated with the user’s personality or possessions.

• Shall safeguard passwords and user account numbers from other personnel by not disclosing them either verbally or in written form. Do not at any time record a password in writing.

• Upon observation of unknown personnel in areas in which sensitive NRC LAN/WAN system data are used or stored, shall challenge them immediately to ensure that their access is authorized.

• Users of NRC AIS property and supplies, including portable computing devices, shall comply with the requirements of MD 13.1, “Property Management,” to ensure that NRC AIS and portable computing devices are protected against loss, theft, or destruction. Because of their portability, security risks to sensitive data on laptop

computers, personal digital assistants (PDAs), cell phones, and other portable computing devices are greater than for stationary systems.

• Shall ensure that essential user data residing on the individual workstation or laptop are backed up at least quarterly and that media containing backup data are relocated to an area physically removed from the workstation.

• Shall scan all files received from external sources for malicious code (viruses) before introducing them to networked NRC systems.

• When leaving a workstation unattended, manually log off the system to prevent access to NRC LAN/WAN system data, or lock the workstation by selecting the appropriate action after pressing the Ctrl-Alt-Delete keys on the keyboard.

• Shall position their workstation monitors to preclude casual viewing of sensitive data during processing.

• Shall ensure that the screen-saver password protection option is selected and the wait time is set to 15 minutes.

• Shall power-off individual workstations at the end of each duty day.

• Shall ensure that user printers are placed in an area in which access can be controlled to ensure that only authorized personnel access sensitive hard copy output. Classified information and SGI shall not be sent through an unclassified LAN server to a printer.

• Shall never copy any classified information or SGI on a copy machine that is connected to the NRC unclassified network.

• Shall never connect to other networks or hosts (via dial-up modems or network connections) without prior permission of NRC IT security personnel.

• Shall seek OIS approval before using personal hardware and software on NRC systems. Any installation of software on NRC systems shall be approved by OIS.

• Shall obtain OIS approval and adhere to software copyright laws before installing software on NRC systems, including standalone personal computers (PCs) and laptops. Comply with software copyright license laws and policies that prohibit unauthorized use or copying of commercial software.

• Shall never attempt to circumvent or defeat security safeguards and countermeasures implemented for the protection of NRC LAN/WAN system data or NRC processing systems.

• Shall comply with NRC processes and procedures for secure dial-in access to NRC AISs. Direct dial-in access to NRC desktops and LAN/WAN system servers is normally not permitted. If such access is required because of special business needs (e.g., remote troubleshooting by vendors or remote access to resident site computers), this access may be approved on a case-by-case basis by the Director of the Information Technology Infrastructure Division, OIS. It is understood that

dial-in access would pose additional security risks but may become necessary for certain job functions.

• Shall ensure that only NRC-authorized Internet connections are being used. All proposed connections shall be authorized and approved by OIS.

• Shall comply with NRC policies related to the personal use of Government IT. MD 2.7 specifies that it is NRC policy to permit employees limited use of agency IT for personal needs if the use does not interfere with official business and involves minimal or no additional expense to the NRC. MD 2.7 defines the acceptable conditions for NRC employees' personal use of IT.