

**Bureau/Agency**

**System Technical Implementation Guideline (STIG)**

**for the**

**Quarters Management Information System (QMIS)**



**National Business Center**  
**March 12, 2008**

**Revision/Change Record**

<b>Revision</b>	<b>Date</b>	<b>Authorization (Optional)</b>	<b>Revision/Change Description</b>	<b>Pages Affected</b>
V 1.00	3/12/2008		Initial Release; 2007 C&A	All

**TABLE OF CONTENTS**

**1 SYSTEM IDENTIFICATION.....1**  
    SYSTEM NAME/TITLE ..... 1  
    RESPONSIBLE ORGANIZATION ..... 1  
    DESIGNATED POINTS OF CONTACT ..... 1  
**2 GENERAL PURPOSE .....2**  
**3 GENERAL DESCRIPTION OF QMIS.....2**  
**4 BOUNDARIES.....3**  
    QMIS MAJOR APPLICATION BOUNDARY ..... 3  
    BUREAU/AGENCY QMIS BOUNDARY..... 5  
**5 PROCEDURES FOR SECURING QMIS.....6**  
    NBC ROLES AND RESPONSIBILITIES ..... 6  
    BUREAU/AGENCY ROLES AND RESPONSIBILITIES..... 8  
**6 NBC RULES OF BEHAVIOR .....10**

# 1 SYSTEM IDENTIFICATION

## System Name/Title

Quarters Management Information System (QMIS)

## Responsible Organization

Quarters Program Office  
Complementary Systems Branch  
Finance & Procurement Systems Division  
Financial Management Systems Directorate  
National Business Center (NBC)  
7301 W. Mansfield Ave., Mail Stop D-2910  
Denver, CO 80235-2230  
Phone: 303-969-5050 Fax: 303-969-6634

## Designated Points of Contact

### System Owner:

Michael Keegan, Associate Director  
Facility & Property Management  
Office of Acquisition & Property Management (PAM)  
Office of the Secretary  
Department of the Interior  
1849 C Street, N.W., Mail Stop 2607-MIB  
Washington, DC 20240  
Phone: 202-208-3347 Fax: 202-219-4244  
E-Mail: Michael\_Keegan@ios.doi.gov

### Program Manager and Acting System Manager:

Douglas Pokorney, Quarters Program Manager  
Quarters Program Office  
Complementary Systems Branch  
Finance & Procurement Systems Division  
Financial Management Directorate  
National Business Center (NBC)  
7301 W. Mansfield Ave., Mail Stop D-2910  
Denver, CO 80235-2230  
Phone: 303-969-5050 Fax: 303-969-6634  
E-Mail: Doug\_B\_Pokorney@nbc.gov

## 2 GENERAL PURPOSE

This document sets forth the minimum controls required to secure a stand-alone desktop application of the Quarters Management Information System (QMIS). It establishes and documents the security roles and responsibilities for participating in the Quarters Program.

There are numerous Federal laws, regulations and policies that apply to asset and property management, housing, rental rates, and Federal employee relations. For example, all Federal Agencies are subject to the requirements of Office of Management and Budget (OMB) *Circular A-45, "Rental and Construction of Government Quarters,"* revised October 20, 1993; their Bureau or Agency housing management policies (DOI Bureaus must follow the "*Departmental Housing Management Handbook*" (DM 400)); and decisions of the National Housing Council. This document does not address all of the requirements to participate in the Quarters Program nor to operate QMIS software.

## 3 GENERAL DESCRIPTION OF QMIS

QMIS provides rental rates for civilian Federal employees living in government-owned or -leased housing. Rent payments are generally deducted from the Federal employee's pay by the organization. QMIS and related rent-setting services are provided under contract by the National Business Center (NBC) Quarters Program in Denver, Colorado. The QMIS application automates the rent-setting process for 6 DOI Bureaus and 14 other Federal Agencies. In total, QMIS is used to set rents for over 20,000 civilian housing units in the U.S. and its territories, the U.S. Virgin Islands, Guam, and American Samoa.

The NBC Quarters Program establishes rental rates for government housing in compliance with *OMB Circular A-45, "Rental and Construction of Government Quarters,"* revised October 20, 1993. Circular A-45 specifies that rental rates for employee/tenants living in government housing be derived from private rental market data. Under the guidance of the Quarters Program, rental rates and other property data are collected by a contractor from the communities nearest to government housing. Surveys are conducted for a given community and region once every four years; during the interim years, national inflation measures are added to rents each March. Private rental market data is statistically analyzed by the Quarters Program staff, and the survey results are published in a report. On average, three or four regions are surveyed each year; there are a total of 16 regions surveyed in the U.S. and its territories. Each year, the QMIS application is updated with new rent formulas for these survey regions, plus inflation measures for all other regions. Each year in January the updated QMIS application is distributed to participating Bureaus/Agencies, then they have the QMIS application installed on their desktop by the Bureau's/Agency's information technology personnel. Employee's rents are adjusted each March, per OMB Circular A-45.

QMIS functions as a distributed, single-user, stand-alone desktop application. The QMIS desktop application provides a graphical user interface through a custom Microsoft Visual Basic executable process. The application interfaces with a stand-alone Microsoft Access database that is stored by the individual QMIS user on their desktop. Both the QMIS application and the Access database are required in order to set rents, and both components are only stored on the user's PC/workstation, never

in a shared environment. The Access database stores the housing inventory, employee/tenant data, and rent calculations for each housing installation the user has responsibility for overseeing. QMIS users at the Bureau/Agency are responsible for the accuracy of their own housing data.

Bureau/Agency QMIS users are also responsible for the calculation and implementation of rental rates; the QMIS application is simply a tool for them to use in this process. Since QMIS does not connect electronically to the NBC IT environment nor any other stand-alone system, employee-tenant payroll deductions for rent must be implemented by Bureau/Agency staff in hard copy or via other internal payroll applications as applicable to the organization. For this reason, personally identifiable information (PII) may exist at the Bureau/Agency for payroll deduction purposes, either in hard copy or electronically. Any PII data is collected directly from Bureau/Agency employee-tenants or employee Supervisors; it is never stored in the QMIS database. Effective with the 2008 application, when the user installs the application as instructed, no PII data can be stored in the user's QMIS database file.

Once a year, in May, each QMIS user sends a copy of their Access database to their regional or national housing manager. National housing managers then submit a copy of the consolidated Bureau/Agency database to the NBC Quarters Program Office. The consolidated national database is used for management and administrative purposes, but more importantly, the data is used to develop the private rental market survey plans. The Quarters Program Office must know where Bureau/Agency housing is located, and what kind of housing exists, in order to survey the individual community rental markets.

## 4 BOUNDARIES

### QMIS Major Application Boundary

The QMIS Major Application (MA) boundary is separate and distinct from each Bureau's or Agency's QMIS boundary.

The QMIS MA boundary, as Certified and Accredited in June 2007, includes only the system components that reside at the NBC Denver campus, such as Quarters Program Office personal computers/workstations, the NBC Local Area Network, and NBC file servers and web servers.

Specifically, the QMIS MA C&A boundary includes:

**Physical Access to the NBC Denver Campus, User Access to NBC Personal Computers, LAN and Servers** – and compliance with other OMB-directed security standards – is managed by NBC Denver Facilities and IT support. All security controls for physical access to the NBC Denver campus, and all security controls for the QMIS MA, are described in the Certification & Accreditation documents, approved in June 2007.

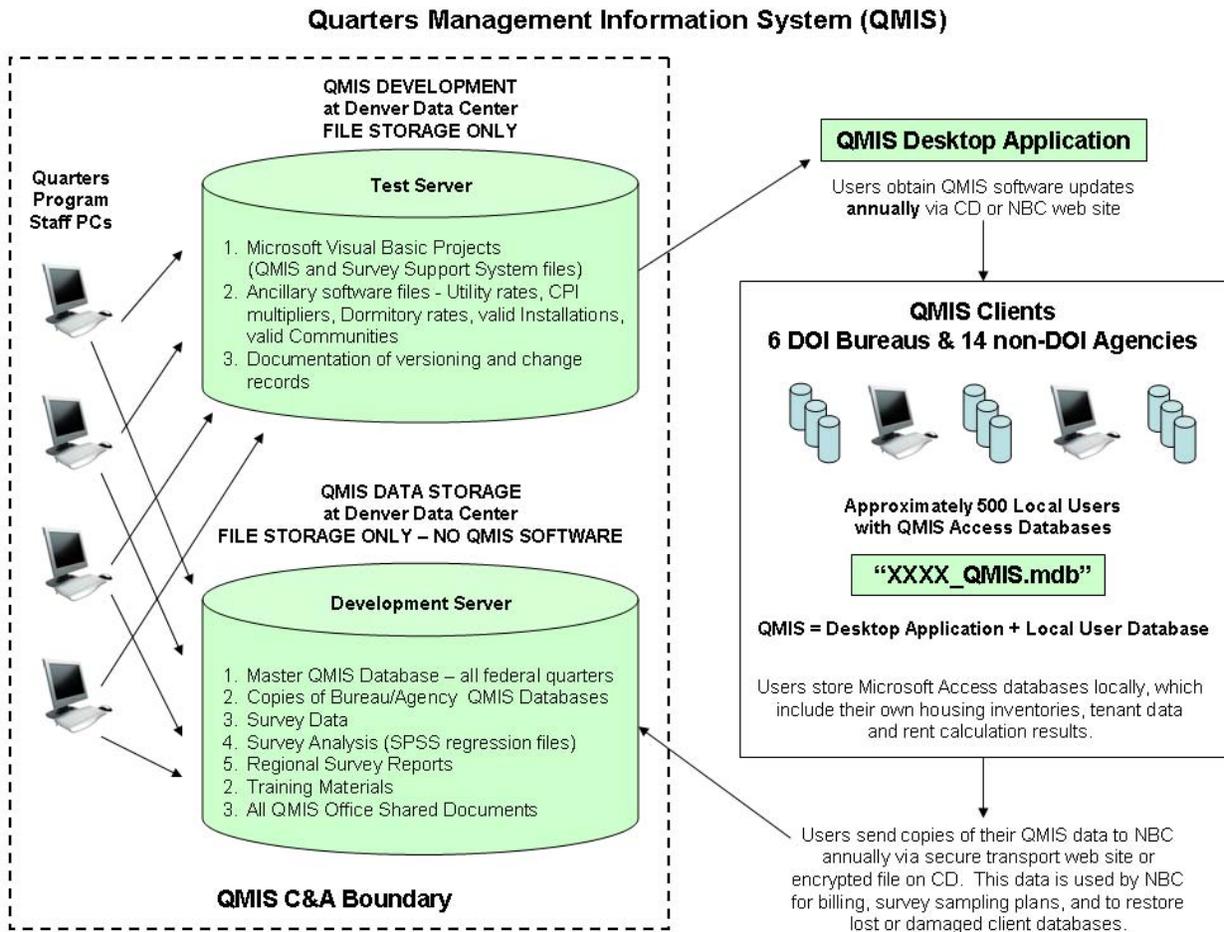
**QMIS Application Programming Files** – Various components of the QMIS application are stored on QMIS servers at the NBC Denver campus. These files include the Microsoft Visual Basic modules and Access databases that are updated and provided to QMIS users each January. Both a shared file server (“production” server) and a survey and software development file server

("test server") are maintained. Physical access and user authentication to these servers is managed by the NBC IT Directorate in Denver, Colorado.

**QMIS Data Files** – Related QMIS files, copies of Bureau/Agency Access databases, a consolidated national Access database, are stored on the Quarters Program servers at the NBC Denver campus. Other files include private rental market data, statistical regression files, survey reports, inflation measures, correspondence, and related administrative files. Physical access and user authentication to this server is managed by the NBC IT Directorate in Denver, Colorado.

**QMIS Program Web Pages and File Transfer Protocol (FTP) Site** – Quarters Program documents and the current QMIS application are available to the public on the Internet, at <http://www.nbc.gov/supportservices/quarter.html>. A secure FTP site is also used to transfer files as needed and instructed by the QMIS Help Desk. NBC web servers are maintained and secured by NBC IT Directorate in Reston, Virginia.

A diagram of the QMIS Environment and C&A Boundary follows:



Since QMIS is not a web-based, client-server application, it requires no inter-connectivity by Bureaus or Agencies. QMIS provides no hosting or centralized processing. No Bureau or Agency needs electronic access to the NBC Denver campus; in fact, any disruptions to connectivity with NBC will have no effect on the user's operability of the QMIS program.

Each Bureau/Agency user installs an updated stand-alone QMIS application on their PC/workstation each January. Each user has their own stand-alone QMIS Access database on their Bureau/Agency PC/workstation or network file server. The QMIS application and database, as stored on each user's computer, is therefore outside of the QMIS MA C&A boundary and is the responsibility of each Bureau/Agency.

The NBC and the Quarters Program cannot provide technical and security compliance functions at Bureau/Agency locations, or on an individual QMIS user's PC or workstation. Therefore, the QMIS C&A boundary is limited to those components physically located at the NBC Denver campus.

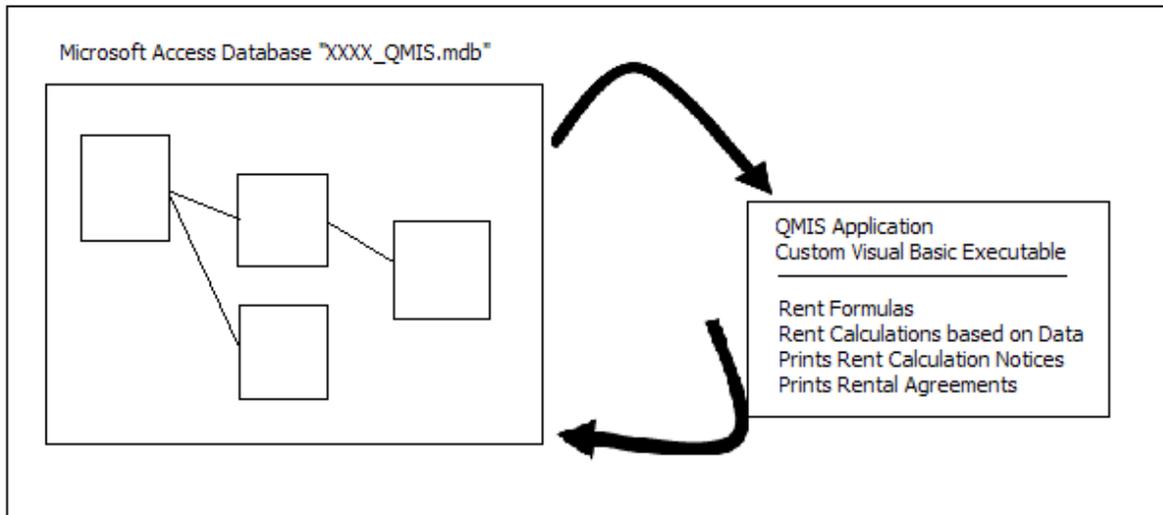
### **Bureau/Agency QMIS Boundary**

Each participating Bureau/Agency is responsible for the physical security and authentication of its employees and contractors, and the security of its own offices, PCs/workstations, LANs and servers. Bureau/Agency employees, PCs/workstations, and QMIS file storage components are therefore within the Bureau's or Agency's boundaries. It is recommended that desktop applications of QMIS, and QMIS database files, be certificated and accredited as part of the General Support System (GSS) of the Bureau/Agency on which it resides.

The diagram below depicts QMIS as it functions on Bureau/Agency PCs/workstations.

#### **QMIS Application and Access Database**

User's Personal Computer Running Windows Operating System



Internet Connection NOT REQUIRED. Application updated annually.

## 5 PROCEDURES FOR SECURING QMIS

### NBC Roles and Responsibilities

1. The NBC will provide technical support and consultation regarding the QMIS system. The QMIS Help Desk (303-969-5696 or 303-969-5050) will generally be staffed between the hours of 6:30 a.m. and 3:00 p.m. MST, Monday through Friday.
2. The NBC will protect all Bureau/Agency data maintained in the consolidated national QMIS Access database, and only disclose it to authorized personnel.
3. The NBC will ensure the QMIS Major Application (MA) is Certified and Accredited in accordance with Office of Management and Budget (OMB) and NIST requirements. Proof of authority to operate (ATO) documents will be provided to the Bureau/Agency on request.
4. The NBC will review and manage security controls at least annually to ensure guidelines are current and enforced (Internal Control Review.)
5. The NBC will ensure that individuals have received background screenings appropriate for their positions using the guidelines established in the *DOI Departmental Manual, Part 441, Personnel Security and Suitability Requirements*.
6. The NBC will evaluate each position description or contract statement of work according to the policies, regulations, and procedural guidelines established in the *DOI Departmental Manual, Part 441, Personnel Security and Suitability Requirements*.
7. The NBC will ensure that employees and contractors read, sign, and return the “Rules of Behavior” (ROB) document. (Section 6 contains the NBC “Rules of Behavior.”)
8. The NBC will ensure that employees and contractors receive initial security awareness training before being given access to NBC-managed computer systems, and annual follow-up security awareness training, as required by *OMB Circular A-130, Appendix III; DOI Departmental Manual 375, Chapter 19*; and the *NBC Computer and Information Security Policy* (NBC-CIO-POL-001).
9. The NBC will ensure that all employees and contractors receive Privacy Information Act awareness training, including how to identify sensitive or restricted information, and how to mark, handle, disclose, release, store, retain, copy or back up, dispose of, sanitize, or destroy such information.
10. The NBC will control physical access to the Denver campus through the use of guards, identification badges, or entry devices such as key cards or biometrics, and ensure keys or other access devices are needed to enter the computer room (the “Denver Data Center”) and/or communication closets.
11. The NBC will ensure that only authorized and authenticated personnel are allowed access to the QMIS PCs/workstations and servers. Access to system software and internal hardware of PCs for system maintenance and repair activities are restricted to authorized users.

12. The NBC will establish and implement procedures for adding new users, updating privileges, removing users, or reducing privileges to facilities and personal computers when hiring, transferring, and terminating staff from the NBC.
13. The NBC enforces the use of individually assigned User IDs and secret passwords that must be changed on a standardized cycle of password aging.
14. The NBC will ensure the QMIS servers are housed in dedicated computer support facilities which provide access control, power conditioning, uninterruptible power service, and environmental controls geared specifically for enterprise server operations.
15. The NBC will routinely monitor physical accesses to QMIS servers through audit trails and manual access logs. The NBC provides a Computer Security Incident Response Capability in the event of a successful penetration attack against an NBC system, and notifies clients whenever a computer security incident occurs that involves or threatens the Bureau's or Agency's application or data.
16. The NBC will ensure that policy and procedures are in place such that apparent security violations are to be investigated and remedial action taken.
17. The NBC will ensure policy exists such that all security issues brought to QMIS Help Desk attention are relayed immediately to the appropriate Bureau/Agency personnel, and to the Bureau/Agency IT Security Manager if necessary.
18. The NBC will ensure QMIS data is protected from interception. This can be accomplished by controlling physical access to communication closets and data transmission lines, and other industry best practices.
19. The NBC will employ network- or host-based Intrusion Detection Systems on the QMIS servers, and monitor it periodically. During times of reported performance issues or suspicious network traffic, the NBC will consider use of packet-level monitoring, which tracks by multiple methods, including MAC address, protocol, IP address, username, and port.
20. The NBC maintains policies and procedures for performing regular data backups, and for storing backups securely, in the event of a disaster or other outage that would require recovery of QMIS files.
21. The NBC will ensure that all QMIS printed output is properly secured or destroyed per regulations.
22. The NBC will ensure that policy exists for control of any media (including backup tapes) generated by QMIS.

## Bureau/Agency Roles and Responsibilities

1. The Bureau/Agency will ensure that individuals have received background screenings appropriate for their positions using the guidelines established in the *DOI Departmental Manual, Part 441, Personnel Security and Suitability Requirements* for DOI personnel and similar regulations, if they exist, for non-DOI staff.
2. The Bureau/Agency will ensure that only authorized and authenticated personnel are allowed access to the QMIS PCs/workstations and servers. The Bureau/Agency will ensure that only authorized housing personnel have access to the QMIS Access database.
3. No user of QMIS will occupy housing. If this situation is unavoidable, then said person will not be allowed to maintain their own inventory data, establish their own rent or submit their own payroll deduction form for rental payments.
4. The Bureau/Agency acknowledges that the QMIS software does not perform identification or authentication of the user before application access is granted. Physical and logical access to the QMIS application and database is the responsibility of the Bureau/Agency.
5. The Bureau/Agency will ensure authorized personnel have received appropriate security awareness training, in accordance with OMB Circular A-130, Appendix III.
6. The Bureau/Agency will authenticate and control access to QMIS PCs and servers through the use of individually assigned User IDs and secret passwords that must be changed on a standardized cycle of password aging.
7. The Bureau/Agency will establish and implement procedures for adding new users, updating privileges, removing users, or reducing privileges to facilities and PCs when hiring, transferring, and terminating staff from the Bureau/Agency.
8. The Bureau/Agency will ensure that all QMIS user's PCs/workstations and servers housing QMIS databases are continually updated, secured and patched to the highest recommended manufacturer standards and/or standards implemented by the DOI Bureau/Agency IT policy. The Bureau/Agency will install and activate virus detection and elimination software.
9. The Bureau/Agency will install the latest version of QMIS each and every year. The Bureau/Agency will provide IT and technical support to its QMIS users, including assistance with installation of the updated QMIS application each January, as needed.
10. Bureau/Agency QMIS users are responsible for the verification and accuracy of the housing inventory in their QMIS Access databases. Rental rates produced by the QMIS application are based on the accuracy of inventory data.

11. The Bureau/Agency understands the QMIS Access database contains all the QMIS inventory data. The Bureau/Agency understands it is their responsibility to safeguard this database. The NBC is not responsible for providing or maintaining this data, should it be damaged or deleted.
12. The Bureau/Agency maintains policies and procedures for performing regular data backups, and for storing backups securely, in the event of a disaster or other outage that would require recovery of the QMIS database files.
13. The Bureau/Agency will provide the NBC Quarters Program Office with a copy of their updated QMIS database annually.
14. The Bureau/Agency will ensure QMIS data files are protected from interception. This can be accomplished by controlling physical access to communication closets and data transmission lines, and other industry best practices.
15. The Bureau/Agency agrees to abide by the DOI “Policy on the Transmission of QMIS Databases” memorandum, dated January 23, 2006, from Debra Sonderman, Director, Office of Acquisition and Policy Management.
16. The Bureau/Agency will authorize the NBC Quarters Program staff to access their QMIS data to the extent necessary to perform normal QMIS operational functions (e.g., for data backup and recovery, reporting purposes, or any other appropriate business needs), as may be required.
17. The Bureau/Agency will ensure that its employees and contractors behave in a manner that is appropriate to the use and protection of the QMIS system and data, based on applicable federal laws, regulations, Bureau/Agency policy, and security guidelines and recommendations.
18. The Bureau/Agency will ensure that policy and procedures are in place such that apparent security violations are to be investigated and remedial action taken.
19. The Bureau/Agency will support employee participation in QMIS training where feasible.
20. The Bureau/Agency will report any system or software flaws to the NBC QMIS Office so they can be researched and remedied if necessary.
21. The Bureau/Agency will report to NBC IT Security any security events or incidents at a Bureau/Agency site that might threaten or negatively impact the integrity or availability of QMIS.
22. The Bureau/Agency will ensure that all QMIS printed output is properly secured or destroyed per regulations. Any payroll- or rent-related printed documents that display personally identifiable information will be kept in a locked and secure storage area, and will be properly maintained and disposed of according to Bureau/Agency retention schedules.

## 6 NBC RULES OF BEHAVIOR



### Rules of Behavior for National Business Center Users of Information Technology Resources



---

These rules are based on Office of Management and Budget (OMB) Circular A-130, Appendix III, Department of the Interior (DOI) Departmental Manual 375, Chapter 19 (375 DM 19), and the NBC Computer and Information Security Policy (NBC-CIO-POL-001). These rules apply to all users of NBC computer systems.

This document establishes a minimum set of rules of behavior while using IT (Information Technology) resources that are owned, leased, or managed by the Department of the Interior (DOI) or the National Business Center (NBC). IT resources include, but are not limited to, computers, networks, data, communications media, transportable data storage media, etc. Managers of Federal and contract employees are responsible for ensuring that these rules are implemented in their organizations and that all users are made aware of their responsibilities. All users are expected to comply with this and referenced DOI and NBC policies and will be held accountable for their actions while using NBC IT systems.

Employees who violate these Rules of Behavior may be subject to disciplinary action at the discretion of the appropriate DOI or NBC management in conformance with the DOI Handbook of Charges and Penalty Selection for Disciplinary and Adverse Actions, DM 752 Handbook 1. Additionally, the local IT Security Manager may remove or disable the user's access to systems in the event of a violation, in accordance with DOI and NBC IT Security policies referenced in these Rules of Behavior.

Network-based systems are inherently insecure and cannot guarantee privacy. In order to underscore this fact, all NBC computer systems display a logon warning banner that states, in part, that:

“Use of this system by any authorized or unauthorized user constitutes consent to monitoring, retrieval, and disclosure by authorized personnel. Users have no reasonable expectation of privacy in the use of this system. Unauthorized use may subject violators to criminal, civil, and/or disciplinary action.”

Because network-based systems are inherently insecure, users should take appropriate measures to protect sensitive information. Refer to the NBC Information Classification Policy, NBC-CIO-POL-003 available on the NBC Web site at <http://www3.nbc.gov/employee/Security/NBC003.pdf>.

## COMPUTER USE

- **National Security Information (NSI Classified Data) may NOT be entered into any NBC computer system.** In the event that National Security Information is accidentally transmitted to an NBC system, the local IT Security Manager must be contacted immediately.
- **NBC and other DOI computer hardware, programs, and data are considered to be the property of the U.S. Government.** Except as allowed by the DOI Policy on Limited Personal Use of Government Office Equipment (available on the DOI Web site at <http://www.doi.gov/ethics/docs/personaluse.pdf>), Government-owned or Government-leased computers, software, and telecommunications systems are to be used for work-related purposes only. Resources are not to be used to conduct or support a personal business; and no personally owned data or software shall be entered into an NBC system, LAN, or personal computer.
- **Unofficial (personal) use of Government-owned IT resources** – As noted above, the DOI Policy on Limited Personal Use of Government Office Equipment spells out the rules and conditions governing personal use of IT resources (e.g., computers, printers, E-mail, Internet, etc). This policy is available on the DOI Web site at <http://www.doi.gov/ethics/docs/personaluse.pdf>. Whenever there is a question or a doubt about the propriety of personal use of any Government-owned IT resource, refer to the DOI Policy on Limited Personal Use of Government Office Equipment or to the local IT Security Manager.

## PASSWORDS AND USER IDS

**Passwords** for all NBC computer systems:

- Are considered private and confidential. Users are prohibited from sharing any of their system passwords with anyone.
- To minimize the risk of having the system compromised as a result of poor password selection, users are responsible for selecting passwords that are difficult to guess. Wherever technically supported, as many as possible of the following password selection criteria should be employed:
  - Passwords must be at least eight or more characters in length.
  - Passwords should contain a mix of both upper and lower case letters.
  - There must be at least one numeric character (0, 1, 2, 3...9).
- New (changed) passwords must not be revisions of an old password. Reuse of the same password with a different prefix or suffix (A, B, C, etc.) is not permitted.
- Dictionary words, derivatives of User IDs, and common character sequences such as "123456" may not be used.
- Personal details such as a spouse's name, license plates, social security numbers, and birthdays should not be used unless accompanied by additional unrelated characters.
- Proper names, geographical locations, common acronyms, and slang should **not** be used.
- If exposed or compromised, passwords must be changed immediately.
- **User Identifiers (User IDs)** are required for all users for access to NBC computer systems. Each user must be uniquely identified. **The User ID possesses privileges that are tailored to the duties of the individual user's job and to the individual user's level of "need-to-know."** Each change in access must be approved.
- If duties or job requirements change, accesses no longer needed must be removed, and new accesses must be requested. Supervisors are responsible for notifying the Security Point of Contact (SPOC) whenever such changes occur so that the user's accesses can be changed to suit the new duty or job requirements.

- When employment terminates, each NBC system to which a user has access must be identified and the access terminated. This is accomplished on the checkout form completed by the user and supervisor on the last day of employment during the exit/clearance process. When employment termination is involuntary, is a result of natural or accidental death, or is caused by any other circumstance that precludes the user from performing the exit/clearance process, then it is the responsibility of the employee's immediate supervisor to expediently provide the notification(s).

**NOTE:** The terms "Security Point of Contact" and "SPOC" refer to any individual who has been delegated security responsibilities for administering user accounts (User IDs, passwords, access authorities, etc.), regardless of platform. When the user is a contractor, the Government responsible manager or Contracting Officer's Representative is the supervisor for the purposes of these Rules of Behavior.

- If problems are encountered with a User ID, the supervisor or SPOC must be contacted.

For details, refer to the NBC Computer and Information Security Policy, NBC-CIO-POL-001, available on the NBC Web site at <http://www3.nbc.gov/employee/Security/NBC001.pdf>.

## **USER ACCOUNTABILITY**

- **Auditing of user access and of on-line activity is tied directly to the User ID.** Users are accountable for all actions associated with the use of their assigned User ID and may be held responsible for unauthorized actions found to be intentional, malicious, or negligent. Each user must protect his/her User ID by:
  - Never allowing another person to use or share his/her logon session. Because the logon session is directly associated with an individual User ID, the user is personally accountable for all actions performed with the User ID.

**NOTE:** In the process of remotely trouble-shooting a difficult customer problem over the telephone, a QMIS or other Help Desk Technician may require the employee to reveal their secret password and explain that the problem cannot be resolved via any other means. Employees who need the assistance of a Technician to solve an IT-related problem are not expected to know whether the advice or request of a Technician is valid or whether the Technician is accurately recording the problem and attempted solutions in the Help Desk log. Therefore, if the employee has any reason to question any aspects of the manner in which the Technician is handling or documenting the situation, he/she should request to speak with the Technician's supervisor before providing their secret password. In any event, if an employee does provide their secret password to the Technician as part of the problem resolution process, the employee is responsible for changing his/her secret password immediately following resolution of the problem.

- Locking the workstation or logging off an active session when leaving the workstation for any reason (e.g., going to a meeting, lunch, restroom, etc.) to prevent unauthorized use of the user's logon session. A password-controlled screensaver is an acceptable means for satisfying this requirement, provided the screensaver is activated before leaving the workstation and the screensaver password complies with the password rules spelled out in the Passwords and User IDs section above.

## **AUTHORIZED ACCESS**

- **Users are responsible for the appropriate use and protection of sensitive information to which they have authorized access.** The use of such information for anything other than "official Government business" is expressly prohibited. Users are responsible for adequately protecting any sensitive or Privacy Act data entrusted to them. Users are prohibited from disclosing, without proper authorization, sensitive or Privacy Act information to individuals who have not been authorized to access the information.

- **Due to the high sensitivity of Individual Indian Trust Data (IITD) and Tribal Trust Data (TTD)**, users must take extra care and precautions to protect any files or data entrusted to them related to IITD/TTD from unauthorized access.
- **Casual browsing of sensitive or Privacy Act information, such as personnel data, is not appropriate and is prohibited.** Users should **only** access this data when there is an official business reason.

For details, refer to the NBC Computer and Information Security Policy, NBC-CIO-POL-001, and the NBC Information Classification Policy, NBC-CIO-POL-003 available on the NBC Web site at <http://www3.nbc.gov/employee/Security/NBC003.pdf>.

## UNAUTHORIZED ACCESS

- **Users are prohibited from accessing or attempting to access systems or information for which they are not authorized.** Users are prohibited from changing access controls to allow themselves or others to perform actions outside their authorized privileges. Users may not imitate another system, impersonate another user, misuse another user's legal user credentials (User IDs, passwords, etc.), or intentionally cause a computer or network component to function incorrectly. Users may not read, store, or transfer information for which they are not authorized.

## DATA PROTECTION

- **Users are prohibited from intentionally adding, modifying, or deleting information or programs** on any NBC computer system or component thereof without a documented and approved form or request for the addition, modification, or deletion.  
**NOTE:** This prohibition is not intended to include user-owned work files on individual workstations or on shared storage devices designated specifically for nonproduction use by individual users or groups. Nor is it a prohibition on user modifications to customizable software features such as "Preferences" or "Options", etc., unless such customization is not allowed by local policies, procedures, or standards. When unsure, users should consult with their supervisor or SPOC.
- **Users who establish individual files** must ensure that security of the files is commensurate with the sensitivity or criticality of their content. Users should contact their supervisors or SPOCs for assistance in protecting individual files.
- **Data requiring protection under the Privacy Act**, proprietary data, other sensitive data or official Agency documents may not be copied or otherwise removed from NBC systems for the purpose of sharing such data outside the authorized user's immediate work group, unless the information sharing has been authorized in writing by the Data Owner. Refer questions regarding Privacy Act information to the Departmental Privacy Officer at (202) 219-0868, or the Office of the Secretary Privacy Officer at (202) 208-6045.

## DENIAL OF SERVICE

- Users may not initiate actions which result in limiting or preventing other authorized users or systems from performing authorized functions by deliberately generating excessive network traffic and thereby limiting or blocking telecommunications capabilities. This prohibition includes the creation or forwarding of unauthorized mass mailings such as "chain letters", or messages instructing the user to "send this to everyone you know", or any messages with excessively large attachments or embedded graphics that consume large quantities of network bandwidth.

## MALICIOUS (HOSTILE) SOFTWARE

- **Users must not intentionally write, compile, copy, propagate, execute, or attempt to introduce** any computer code designed to self-replicate, damage, or otherwise hinder the performance of any DOI or NBC computer system. Examples of these would be computer viruses, worms, and Trojan horses. For details, refer to the NBC Computer and Information Security Policy, NBC-CIO-POL-001, available on the NBC Web site at <http://www3.nbc.gov/employee/Security/NBC001.pdf>.

## BYPASSING SYSTEM SECURITY CONTROLS

- **Unless specifically authorized by the NBC IT Security Manager**, NBC workers must **not** acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls. Examples of such tools include those that defeat software copy protection, discover (crack) secret passwords, or identify security vulnerabilities, etc. Additional examples include employing specialized system software mechanisms to bypass system security controls as a convenience measure.
- **Workers must not test or probe security mechanisms** at either the NBC or external installations unless they have first obtained permission from the NBC IT Security Manager.

## COPYRIGHT LAWS AND LICENSE REQUIREMENTS

- **Commercially developed software.** Commercially developed software must be treated as the proprietary property of its developer. Title 17 of the U.S. Code states that it is illegal to make or distribute copies of copyrighted material without authorization. The only exception is the user's right to make a backup for archival purposes assuming the manufacturer does not provide one. It is illegal to make copies of software for any other purposes without the written permission of the copyright owner. Making or using unauthorized copies of copyrighted products from a DOI or NBC computer system is illegal and is expressly prohibited.
- **DOI and NBC-owned computer systems.** Users may only install commercial software that is acquired through an approved DOI or NBC procurement process. Vendor licensing requirements must be followed.
- **Personally owned software.** Users may not install personally owned software on DOI or NBC-owned computer systems. This includes but is not limited to personally owned screensaver software. An employee who has any doubt as to the appropriateness of installing personally owned software on a DOI or NBC-owned computer system should check with his or her supervisor for guidance.

## CONNECTING TO THE INTERNET

- **NBC personnel are provided with the equipment and Internet connection to accomplish the work of the NBC.** Limited personal use of the Internet is governed by the DOI Policy on Limited Personal Use of Government Office Equipment (available on the DOI Web site at <http://www.doi.gov/ethics/docs/personaluse.pdf>.) Workers on **nonduty** time are allowed to use the Internet for personal use in accordance with the DOI Internet Acceptable Use Policy (available on the DOI Web site at <http://www.doi.gov/ethics/docs/internet.html> ). Except as prohibited by the DOI Internet Acceptable Use Policy, workers are allowed minimal personal purchases through the Internet, but only during nonduty time. Nonduty time is determined by DOI and NBC management and is limited to official breaks, lunch, and before and after duty hours. When making such purchases, however, employees must arrange for the purchases sent to a non-Government address. Employees are prohibited from using Government office equipment at any time to make purchases for personal commercial gain activity. The prohibited activities listed in the DOI Internet Acceptable Use Policy include but are not limited to:
  - Using Government-provided access to the Internet to present their personal views in a way that would lead the public to interpret it as an official Government position.

- Using the Internet as a radio or music player (e.g., use of “streaming audio or video”).
- Using “push” technology on the Internet or other continuous data streams, unless they are directly associated with the employee’s job.
- Using Government-provided E-mail for personal use except as authorized by Departmental policy as referenced in these Rules of Behavior.
- Using Government office equipment at any time for activities that are illegal (e.g., gambling) or that are inappropriate or offensive to co-workers or the public, such as the use of sexually explicit material, material or remarks that ridicule others on the basis of race, creed, religion, color, sex, disability, age, national origin, or sexual orientation.

## RECORD RETENTION REQUIREMENTS

- **Users must follow DOI and NBC records management policies** (available on the DOI Web site at <http://www.doi.gov/ocio/records>). Any documents or E-mail created may be considered Federal records that must be preserved by being printed and filed and may not be deleted from the system before being saved in the system’s backup process.
- **Record Retention Requirements for Cobell v. Norton litigation.** Users must print and file, in accordance with applicable Court and Departmental directives, any documents they have or create and any E-mail messages they send or receive, including attachments, that relate to the three functional areas of:
  - American Indian Trust Reform, including the High-Level Implementation Plan or any of its subprojects;
  - The Cobell v. Norton litigation; or
  - Administration of Individual Indian Money (IIM) accounts.

## COMPUTER SECURITY INCIDENTS

- **Users and management are required to report all computer security incidents** (viruses, intrusion attempts, system compromises, offensive E-mail, inadequate protection of sensitive data, etc.) to their local IT Security Manager as follows:

● Denver	● (303) 969-7126
● Reston	● (703) 390-6726
● Main Interior Building	● (703) 390-6726
● Boise	● (208) 433-5050

- For additional assistance, users may contact the NBC Customer Service Center (CSC) at (303) 969-7777.
- **Users are responsible for cooperating with NBC IT System Administration and IT Security staff and the local IT Security Manager** during the investigation of a computer security incident.

## USER RESPONSIBILITY

- **Users are responsible for following all the general computer use and IT security rules included in these Rules of Behavior** and for implementing appropriate controls to protect the resources and information under their control (as described in policies referenced in these Rules of Behavior). Each local NBC

organizational unit or system may require additional levels of security controls. Resources permitting, users are responsible for implementing controls as requested by the local IT Security Manager.

- **Individual accountability.** Users will be held accountable for their actions on DOI and NBC IT systems. If a user adversely impacts the operation of a DOI or NBC IT system, the employee's access may be removed without notice to ensure the operation and availability for the rest of the system users.
- 
-

**INDIVIDUAL COMPUTER USER'S  
ACKNOWLEDGEMENT OF RESPONSIBILITY  
FOR USE OF NBC COMPUTER SYSTEMS**

I understand that when I use any of the National Business Center's computer systems or Information Technology (IT) resources or gain access to any information therein, such use of access shall be limited to official Government business (except as allowed by the DOI Policy on Limited Personal Use of Government Office Equipment, available on the DOI Web site at <http://www.doi.gov/ethics/docs/personaluse.pdf> ). Further, I understand that any use of the aforementioned systems or information that violates these Rules of Behavior may result in disciplinary action consistent with the nature and scope of such activity.

**NOTE:** Security policy infractions committed by contractors or vendors who are working for, and being paid by, the National Business Center will be handled in accordance with the provisions of their respective contracts concerning disciplinary or punitive actions, except in the case of criminal acts, which will be turned over to local law enforcement or Federal investigators.

I have been provided with and have read the "Rules of Behavior for National Business Center Users of Information Technology Resources". I understand these Rules of Behavior and agree to comply with these Rules.

Print Full Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Federal Employee:

NBC Office: \_\_\_\_\_

Date: \_\_\_\_\_

Contractor:

Company Name: \_\_\_\_\_

Date: \_\_\_\_\_

\_\_\_\_\_