U.S. Department of the Interior's Federal Information Systems Security Awareness Online Course

Rules of Behavior

Before you print your certificate of completion, please read the following Rules of Behavior and press the "ACCEPT & PRINT CERTIFICATE" link below to acknowledge your acceptance of this statement.

In accordance with the Office of Management and Budget (OMB) Circular A-130, BIA's systems must have a set of rules established to govern the use of and behavior within the system. These rules clearly must delineate responsibilities and expected behavior of all individuals with access to this system. The rules of behavior contained in this document are to be followed by all users. Users will be held accountable for their actions. Employees who violate BIA's policy regarding rules of behavior may be subject to disciplinary action at the discretion of BIA's management. Actions may include a verbal or written reprimand, removal of system access for a specific period of time, reassignment to other duties, or termination depending on the severity of the violation. This document establishes a minimum set of rules of behavior that apply to all BIA and contractor employees who access any BIA computer, computer system application or general support system.

1. General

National Security Information (NSI Classified Data) will not be entered into the system.

All BIA systems require a high degree of protection because they contain, store, and manipulate large amounts of sensitive, private, and financial information for Indians and tribes. The general rules of behavior are:

a. All individuals who access any BIA system must be aware of the sensitivity of its data. They must be aware that any intentional corruption or falsification of this data will result in disciplinary action.
b. Each user accessing any BIA system must have unique user identification (USERID) and a strong password for accountability reasons. Users are responsible for all actions performed under their user account ID.
c. Users will be held accountable, individually, for their actions.
d. Each user will be assigned to only one agency, activity, or office. Users will not attempt to log in to different departments or accounts.
e. Users will be assigned only the access rights or privileges needed to perform their tasks. Users are given access to BIA systems based on a need to perform specific work. Users are to work within the confines of the access allowed, and are not to attempt to access data, applications, or systems for which access has not been authorized.
f. Management must request a new user account or additional access rights or privileges for a user. Management must notify the system owner and the system

administrators whenever there is a change in the employment status or roles and responsibilities of their subordinates.
g. The system owner must approve supervisors' request before an account can be created.
h. Users are not authorized to assign their own access rights. Only account managers and designated IT specialists will have the authority and tools to implement assignment of user access rights and permissions.

2. BIA's Information Technology Security Manager (BITSM)

The BITSM is responsible for ensuring that an adequate level of protection is afforded information systems, through an appropriate mix of technical, administrative, and managerial controls. To protect the security of BIA sensitive data, the BITSM will:

a. Be appointed in writing.
b. Develop computer security policies and procedures for BIA systems.
c. Develop and conduct employee and contractor awareness sessions.
d. Conduct inspections and spot checks to determine that an adequate level of compliance with security requirements exist.
e. Conduct periodic vulnerability analyses to help determine if security controls are adequate, given the ever-changing nature of security threats environment. Special attention must be given to new and developing technologies, systems, and applications that can open, or have opened vulnerabilities in BIA's security posture.

3. System Administrator (SA)

The SA is responsible for the daily operations of the system. To protect the security of BIA's sensitive data, the SA will:

a. Perform routine maintenance of database and application servers.
b. Ensure that proper equipment and resources are available to operate the system.
c. Provide administrative advice and assistance on BIA systems to all levels responsible for supporting or managing the system.
d. Ensure that security requirements are considered in a timely and comprehensive manner, while exercising responsibility for planning, designing, and testing the system.
e. Ensure that hardware, cabling and wiring conform to local fire and safety codes.
f. Ensure that standard hardware and software configurations are maintained on servers.
g. Manage change controls and ensure that change control procedures are in use.
h. Manage configuration control for servers and applications. This includes identifying the specific location of all wiring and equipment connected to the servers and workstations.
i. Perform centralized data management to provide regular tape backups in accordance with BIA's policy, or ensure that equivalent procedures are in place.
j. Create new accounts and modify the rights and privileges of existing accounts only if approved by the System Owner
k. Ensure that no combustible or flammable materials are stored inside data center rooms.
l. Perform routine reviews of audit logs to identify suspicious activities.
m. Report all security incidents to the Service Center.

4. Herndon Data Center Manager

The Herndon Data Center manager is responsible for maintaining the security of computer and communication resources housed in the data center and the security of the UPS system. To protect the security of BIA's sensitive data, the data center manger will:

a. Protect the confidentiality, integrity, and availability of all data center resources.
b. Request update of SSPs when significant changes to the Herndon data center occur.
c. Report all security incidents to the BIA Computer Incident Response Team (CIRT) and the Office of Information Security and Privacy.
d. Implement procedures to ensure that there is continuity of service.
e. Follow all authorized and published procedures for securing BIA System operations.
f. Ensure that contingency plans are implemented, tested, and that all individuals involved in the plan know their respective duties and responsibilities concerning the execution of the plan.
g. Manage the daily operation and maintenance of the data center.
h. Manage and control user access to data center resources. User access and privilege levels on any system will be limited to application menus and database files required for job performance.
i. Ensure that data center and Help Desk workstations are equipped with correct and current versions of networking software.
j. Ensure that operators and administrators know whom to contact to report security incidents.
k. Ensure that system level backups are performed regularly and verified for completion.

5. Users

All users (both BIA and contractor employees) are responsible for the secure use of any BIA system. Only personnel approved to work on a specific system shall be provided with access to the system. To protect the security of BIA's sensitive data, all users will:

a. Not attempt to view, change, or delete data, unless authorized to do so.
b. Not use system privileges to obtain data/files or run applications for anyone who is not authorized to do so.
c. Safeguard the use of BIA Systems
d. Attend initial security training and annual refresher training. All users will implement security instructions as directed by the Office of Information Security and Privacy (OISP) or by supervisory personnel.
e. Be aware of the identity, roles, and responsibilities of BIA and contractor personnel responsible for the security of sensitive data.
f. Report security-relevant events to supervisors, the Service Center, the OISP or BIA CIRT. This includes security infractions by co-workers, attempted access by unauthorized personnel, violations of procedures, disclosure of sensitive information, loss of availability of resources, destruction of data, or detection of erroneous information or unexplained system activity.
g. Provide immediate notification to supervisory personnel when a decision is made to retire, resign, transfer, or otherwise change the basis for which your access to the system has been granted.
h. Select secure passwords, which are non-dictionary character strings, at least eight characters in length, are a combination of both numbers and characters, and which cannot be associated easily with the user. Passwords must be changed at least every 90 days. The reuse of passwords is prohibited.
i. Safeguard passwords and user account numbers from other personnel by not disclosing them either verbally or in written form. Users will not, at any time, share or display their passwords. Users will not, at any time, record a password in writing.
j. Never discuss or otherwise reveal sensitive information that should not be disclosed to unauthorize personnel either over the phone, in face-to-face discussions, or in an area where unauthorized personnel might overhear conversations involving sensitive information. This is especially true for personal information subject to the Privacy Act.

k. Safeguard sensitive hard copy data and reports (particularly reports containing Privacy Act data) when not attended by securing it in a locked office or secured desk or cabinet. When printing hard-copy output containing sensitive data at a printer accessible to unauthorized personnel, pick-up the printed material in timely manner to ensure that unauthorized personnel cannot view or obtain the output. If not already labeled, mark all screen print-outs and hard-copy output containing Privacy Act information as “Sensitive Information”. Mark it with an indication that the output contains data subject to the Privacy Act of 1974, and that it should be withheld from disclosure to unauthorized personnel. Destroy sensitive documents and reports by burning or shredding.

l. When copying sensitive information to electronic media, label the media with an indication that the output contains sensitive information and that it should be withheld from disclosure to unauthorized personnel.

m. Access only the data which is necessary to perform assigned duties, and report failures in the system's access control mechanism to supervisory personnel. Also, notify supervisory or security personnel when authorized access rights and privileges are no longer required.

n. No trust data or screens will be saved to the user’s workstation or to a floppy diskette. Users may retrieve, browse, modify, copy, or delete only those files that they were authorized to. Users will ensure that they have been given the appropriate privileges (such as read, write, execute, modify, or delete) before working with any files. Users are not allowed to delete records without proper and written authorization from the information owner.

o. Password protected screen savers shall be automatically activated after 5 minutes of user inactivity. Users shall be able to activate the password protected screen saver at will. Users shall activate the screen saver with a password whenever they leave their workstations unattended.

p. Users shall ensure that only authorized personnel can view sensitive information that they have retrieved, whether the information is on the user’s screen or on paper. When viewing or processing sensitive information, users’ screens must be positioned away from doors, windows, and areas accessible to unauthorized personnel or visitors.

q. Unknown personnel, in areas where sensitive data is used or stored, should be challenged immediately to ensure that their access to sensitive data is prevented.

r. Strive for total accuracy during data input. Upon discovery of errors or bad data, either correct the inaccurate data or notify supervisory personnel of its existence.

s. Follow all virus protection procedures. Do not tamper with virus protection software installed on the desktop. Know how to use virus scanning software. Scan all new software or diskettes/CDs received, such as shared document disks or mail attachments, for malicious code (viruses) prior to opening them or storing them on a workstation. Use only legal copyrighted software and avoid inexpensive software or shareware from uncertain sources. If a user receives a “virus hoax,” the user should report the suspected virus hoax to the service center, the OISP, or BIA CIRT. Users will not perpetuate the virus hoax or send it to anyone else. Users will delete the virus hoax.

t. DO NOT establish multiple login sessions.

u. Manually log-off the system to prevent access to sensitive data when leaving a workstation unattended, especially with any Intranet, e-mail, or major application open. Always use the proper shut down command to shut down the computer.

v. Log-off individual workstations at the end of each workday.

w. Ensure that individual workstations and peripheral devices are connected to a surge suppressor or other power protection device.

x. Protect system hardware from hazards, such as water or excessive heat. To safeguard system hardware, avoid placing beverage containers or food near or on top of a workstation. No food or drinks are allowed near any of BIA’s servers.

y. Never connect to other networks or hosts without prior permission from BIA's supervisory or security personnel.
z. Any hardware, software, and data on a BIA System is the property of the U.S. Government. Use BIA's equipment and data for official purposes only.
aa. Use BIA's mail system and the Intranet for official purposes only. Periodic review of system usage by individual users for appropriateness of use will be conducted. Users of BIA e-mail must understand that they have no inherent right to privacy. Users of BIA e-mail also must understand that any e-mail originating or received in BIA is subject to the Freedom of Information Act.
bb. Use BIA's portable equipment (i.e., laptops, etc.) for work-related purposes only.
cc. Seek supervisory approval before requesting the installation or use of any hardware or software on BIA owned computers. Loading or using personal hardware and software is prohibited and may cause viruses or compromise security.
dd. Adhere to software copyrights and seek supervisory approval before requesting the installation of BIA-provided software on personal computer systems. "Software" includes any software for screen savers, communications packages, database management, word processors, spreadsheets, graphics, specialized applications, etc. BIA requires that all copyright licenses for PC-based and LAN-based software, used by BIA's employees and contractors, be understood and that personnel comply with the license requirements. End users, supervisors, and function managers are ultimately responsible for compliance. Users will not at any time install any software, licensed or un-licensed, on their workstations. Software diskettes, license agreements, and software manuals are to remain in the office.
ee. Audit logs will be reviewed periodically to determine whether users, without authorized access privileges, attempt to access BIA servers on which valuable, off-the-shelf software resides. Audit logs also will show users' use of a "copy" command, which may indicate attempts to illegally download software.
ff. Never attempt to circumvent security safeguards and countermeasures implemented for the protection of sensitive BIA data or processing systems.
gg. Never remove sensitive data from any BIA facility without the prior approval of supervisory personnel.

6. Dial-up Access

The CIO may authorize dial-up access to the BIA's network or a system. It is understood that dial-up access poses additional security risks, but it may be necessary for certain job functions. If dial-up access is allowed, the OISP will review the telecommunications logs and BIA phone records regularly, and conduct spot-checks to determine if BIA organizational units are complying with controls placed on the use of dial-up lines. All dial-up lines will use separate USERIDs and passwords.

7. Connection to the Internet

All BIA system users should know that only authorized Internet connections will be allowed, and that all connections must conform to BIA's security and communication architecture. BIA should ensure that the user authentication required for access is adequate to protect user's programs and data. When such access is allowed, BIA should document all external connections to ensure that access to BIA's network is limited to controlled points of entry.

8. Restoration of Service

The availability of BIA systems is a concern to all users. Generally, users are responsible for only ensuring the restoration of their services in the event resources in the Herndon Data Center are not operational. Data restoration is addressed by performing incremental backups on a daily basis and a full system backup of their data on at least

on a weekly basis. If data becomes corrupted for any reason, it will be fully recoverable up to the point of the last backup.

9. Sanction of Misuse

In accordance with 370 DM 752.1 personnel are individually responsible for protecting the confidentiality, availability, and integrity of data and information accessed, stored, processed, and transmitted. Individuals are accountable for actions taken on and with BIA IT resources and information. Failure to comply with this policy may lead to disciplinary action, as appropriate. Unauthorized disclosure of sensitive information may result in criminal or civil penalties.

I acknowledge that I have received the rules of behavior; I understand my roles and responsibilities and will comply with the rules of behavior.

Name _____

Signature _____ **DATE** _____