Information Systems Security Awareness (ISSA) FY18

IHS Rules of Behavior

The IHS Rules of Behavior (RoB) provide common rules on the appropriate use of IHS information technology resources for all IHS users, including federal employees, contractors, and other system users. Users must review and electronically acknowledge the RoB annually as part of the IHS Information Systems Security Awareness (ISSA) training.

Procedures in this section are the minimum RoB for all users and must be followed by anyone requesting any type of access to IHS systems. Users should realize that these RoB apply even if they do not take the time to read them. By electronically acknowledging, users reaffirm their knowledge of, and agreement to adhere to, the IHS RoB. The IHS RoB cannot account for every possible situation. Therefore, where the IHS RoB does not provide explicit guidance, personnel must use their best judgment to apply the principles set forth in the standards for ethical conduct to guide their actions.

Noncompliance with the IHS RoB may be cause for disciplinary actions. Depending on the severity of the violation and upon management discretion, consequences may include one or more of the following actions:

- Suspension of access privileges
- Revocation of access to federal information, information systems, and/or facilities
- Reprimand
- Termination of employment
- Removal or disbarment from work on federal contracts or projects
- Monetary fines
- Criminal charges that may result in imprisonment

Supplemental RoB may be stipulated for specific systems. Users who access those systems must follow the system-specific RoB in addition to the rules contained in this document. In such cases, users must also accept the supplemental RoB prior to receiving access to these systems and must comply with ongoing requirements of the system to retain access (i.e., re-acknowledging the system-specific rules by signature each year). System owners must document system-specific RoB and any recurring requirement to sign the respective acknowledgement in the Security Plan for their systems.

These IHS RoB apply to local, network, and remote use of IHS information (in both electronic and physical forms) and information systems by any individual.

Users of IHS information and systems must acknowledge the following statements:

I assert my understanding that:

- Information and system use must comply with U.S. Dept. of Health and Human Services (HHS) and IHS policies and standards, and with applicable laws.
- Use for other than official, assigned duties is subject to the IHS Indian Health Manual (IHM) Policy Part 8, Chapter 6: Limited Personal Use of Information Technology Resources.
- Unauthorized access to information or information systems is prohibited.
- Users must prevent unauthorized disclosure or modification of sensitive information.

I Must:

General Security Practices

- Follow IHS security practices whether working at my primary workplace or remotely.
- Accept that I will be held accountable for my actions while accessing and using IHS information and information systems.
- Ensure that I have appropriate authorization before installing and using software, including downloaded software on IHS systems, and before doing so I will ensure that all such software is properly licensed, approved, and free of malicious code.
- Wear an identification badge at all times in federal facilities, except when it is being used for system access.
- Lock workstations and remove Personal Identity Verification (PIV) cards from systems when leaving them unattended.
- Use assigned unique identification and authentication mechanisms, including PIV cards, to access IHS systems and facilities.
- Complete security awareness training prior to accessing an IHS system, and then complete it on an annual basis thereafter, and also complete any specialized role-based security or privacy training commensurate with my duties.
- Permit only authorized IHS users to use IHS equipment and/or software.
- Take all necessary precautions to protect IHS information assets (including but not limited to hardware, software, personally identifiable information [PII], protected health information [PHI], and federal records [media neutral]) from unauthorized access, use, modification, destruction, theft, disclosure, loss, damage, or abuse, and treat such assets in accordance with any information handling policies.
- Immediately report to the local Information Systems Security Officer (ISSO) or the IHS Cybersecurity Incident Response Team (CSIRT) all lost or stolen IHS equipment, known or suspected security incidents, known or suspected information security policy violations or compromises, or suspicious activity.
- Use only approved methods for accessing IHS information and information systems.
- Notify my supervisor or the IT department if access to resources exceeds what is actually needed to perform the job assigned (i.e., if access violates the Least Privilege Policy).
- Obtain approval before using large email distribution lists.
- Use caution with all emails or attachments if I suspect the message is not authentic (e.g., from suspicious sources or with unusual subject lines).
- Maintain awareness of risks involved with clicking on email or text message web links.
- Show courtesy and basic email etiquette when conducting business through email.
- Follow Records Management policies and guidelines for storing and archiving email and its contents. For more information, contact your local IHS Records Management Officer.
- Be aware when navigating through the Internet. It is possible to unknowingly navigate from an area of controlled access into an area of unknown security controls.
- Use only IHS-approved Instant Messaging (IM) systems.

Privacy

- Understand and consent to having no expectation of privacy while accessing IHS computers, networks, or email.
- Collect information from members of the public only as required by my assigned duties and permitted by the Privacy Act of 1974, the Paperwork Reduction Act, and other relevant laws.
- Release information to members of the public, including individuals or the media, only as allowed by the scope of my duties and the law.
- Refrain from accessing information about individuals unless specifically authorized and required as part of my assigned duties.
- Use PII and PHI only for the purposes for which it was collected and consistently with conditions set forth by stated privacy notices such as those provided to individuals at the point of data collection and published System of Records Notices.
- Ensure the accuracy, relevance, timeliness, and completeness of PII, as reasonably necessary and to the extent possible, to assure fairness in making determinations about an individual.

Sensitive Information

- Treat computer, network, and web application account credentials as private sensitive information and refrain from sharing accounts.
- Adequately protect any sensitive information entrusted to me.
- Secure sensitive information (on any medium) when left unattended.
- Keep sensitive information out of sight when visitors are present.
- Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed, in accordance with IHS sanitization and disposal procedures or as otherwise lawfully directed by management.
- Access sensitive information only when it is necessary to perform job functions (i.e., need-to-know).

- Properly protect (e.g., encrypt) IHS-sensitive information at all times while stored or in transmission, including sensitive information sent via email.

Password Standards

- Ensure that passwords:
    - Do not contain common words found in any dictionary.
    - Do not incorporate personal data elements (e.g., user's name, date of birth, address, telephone number, or Social Security number; names of children, spouses, favorite bands, sports teams, pets, or automobiles).
    - Are changed immediately in the event of known or suspected compromise, and immediately upon system installation (i.e., change default or vendor-supplied passwords).
    - Are committed to memory or stored in a secure place.
    - Are not posted or shared with others.
    - Are not the same passwords used for external, personal accounts.

I Must Not:

- Share or disclose sensitive information except as authorized and with formal agreements that ensure third parties will adequately protect it.
- Violate, direct, or encourage others to violate IHS policies and procedures.
- Reconfigure equipment, software, or computers; circumvent the antivirus, firewall, or other security controls or safeguards of the system; or override technical or management controls, except as authorized.
- Use another person's account, identity, password/passcode/PIN, or PIV card or share my password/passcode/PIN.
- Remove data or equipment from the agency premises without proper authorization.
- Use IHS information, systems, and hardware to send or post threatening, harassing, intimidating or abusive material about others in public or private messages or forums.
- Exceed authorized access to sensitive information.
- Transport, transfer, email, remotely access, or download sensitive information unless such action is explicitly permitted by the manager or owner of such information and appropriate safeguards are in place per IHS policies concerning sensitive information.
- Use sensitive information for anything other than the purpose for which it has been authorized.
- Access information for unauthorized purposes.
- Use sensitive IHS data for private gain or to misrepresent myself or IHS or for any other unauthorized purpose.
- Store sensitive information in public folders or other insecure physical or electronic storage locations.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information.
- Copy or distribute intellectual property—including music, software, documentation, and other copyrighted materials—without written permission or license from the copyright owner.
- Modify or install software without prior management approval as outlined in IHS procedures.
- Conduct official government business or transmit/store sensitive IHS information using non-authorized equipment or services.

- Use systems (either government issued or nongovernment) to access sensitive IHS information without the following protections in place:
    - Antivirus software with the latest updates;
    - Antispyware and personal firewalls;
    - A time-out function that requires re-authentication after no more than 30 minutes of inactivity on remote access; and
    - Approved encryption to protect sensitive information that is stored on recordable media, including laptops, universal serial bus (USB) drives, and external disks, or that is transmitted or downloaded via email or remote connections.
- Use network monitoring, cracking, or hacking tools unless specifically authorized in writing to do so as part of job duties.
- Attempt to break into or introduce malicious code into someone else's electronic device or voicemail account.
- Use personally owned information systems or portable media for official U.S. Government business involving the processing, storage, or transmission of federal information, without explicit approval in writing (such use must be in accordance with IHS procedures related to personally owned information systems and software).
- Use a personal email system (e.g., Gmail, Yahoo) or a social media platform to transmit sensitive information.
- Use government systems or networks for games, chat rooms, auctions, gambling, or other personal or nonproductive use, except as permitted by IHS policy.

When using federal government systems, I must refrain from the following activities, which are prohibited per the IHS Policy Part 8, Chapter 6: Limited Personal Use of Information Technology Resources:

- Unethical or illegal conduct.
- Sending or posting obscene or offensive material.
- Sending or forwarding chain letters, email spam, inappropriate messages, or unapproved newsletters and broadcast messages.
- Sending messages supporting prohibited partisan political activity as restricted under the Hatch Act.
- Conducting any commercial or for-profit activity.
- Using Peer-to-Peer (P2P) software except for secure tools approved in writing by the IHS CIO to meet business or operational needs.
- Sending, retrieving, viewing, displaying, or printing sexually explicit or suggestive text or images or other offensive material.
- Creating and/or operating unapproved websites.
- Allowing personal use of IHS resources to adversely affect IHS systems, services, and co-workers (such as using non-trivial amounts of storage space or bandwidth for personal digital photos, music, or video).
- Using the Internet or IHS workstations to play games or gamble.

  Posting IHS information to external newsgroups, social media and/or other types of third-party website applications, or other public forums without authority, including information which is at odds with IHS missions or positions. This includes any use that could create the perception that the communication was made in my official capacity as a federal government employee, unless I have previously obtained appropriate IHS approval.

I Accept the IHS Rules of Behavior

Name _____ **Date** _____

Position Title _____

Supervisor Name: _____

Reference: 2018 IHS ISSA Training, Acknowledgement and Acceptance of the IHS Rules of Behavior
https://www.ihs.gov/ISSA/index.cfm?module=home&option=index