

United States Coast Guard
Polar Science Systems
Coast Guard Polar Science Program

Information System Rules of Behavior
Polar Science Information Infrastructure

EFFECTIVE DATE: 24 January 2012

1. EXECUTIVE SUMMARY

This policy is to help define general acceptable and prohibited behaviors. Underway connectivity is limited and must be managed properly. The security of the network is critical, and the onboard technician may take appropriate action to secure the network. The deployed ESU technician should be contacted for any onboard assistance. Contact information is provided during the welcome aboard brief for Science party members. Additional information on the management of the Polar Science Network is available in the pre-cruise message and welcome aboard brief, in addition to that provided at www.icefloe.net.

2. GENERAL INFORMATION

The U.S. Coast Guard provides information systems for the purpose of transacting official business of the Polar Science Program. The USCG establishes Rules of Behavior for the proper use of these systems. Any non-program use of Polar Science information resources must be authorized by USCG Science network management. The U.S. Coast Guard has created these Rules of Behavior to guide users, content providers and system administrators in the appropriate and acceptable use of Polar Science information resources. This document applies to all information resources that comprise the Polar Science information infrastructure and to all users of these information resources. In this document, the term “you” or “your” refers to the User. The term “User” also includes Content Providers and Systems Administrators.

The Polar Science information infrastructure is a federal government information system composed of several interrelated information systems owned by, and operated for, the U.S. Coast Guard. A significant portion of Polar Science activities take place at remote or isolated locations managed by the U.S. government. Private sector support infrastructure is not available for the personal use of program participants at these locations. Consistent with federal guidelines for management of agency resources, Polar Science information systems may be used for morale and welfare purposes as deemed appropriate by program management. Information maintained in USCG systems, including electronic mail files, may be reviewed by USCG officials who have a legitimate reason to do so when authorized by U.S. Coast Guard management. Unauthorized attempts to modify any information stored on this system, to defeat or circumvent security features, or to use this system for other than its intended purposes are illegal and may result in disciplinary action, criminal prosecution, or both.

Where applicable; Polar Science information resource users must comply with USCG policies and procedures, as well as your own organization’s policies and procedures governing the personal use of USCG government equipment. In the event of a conflict, the USCG policies and procedures, including these Rules of Behavior, take precedence. These Rules of Behavior apply to all users of

the Polar Science information infrastructure whether you are a USCG employee or not. Polar Science information resource users must comply with these Rules of Behavior. Because written guidance cannot cover every contingency, you are asked to go beyond the stated rules, using your best judgment and highest ethical standards to guide your actions. These Rules are based on Federal laws and regulations and agency directives. As such, there are consequences for non-compliance. Depending on the severity of the violation, at the discretion of management and through due process of the law, consequences can include: suspension of access privileges, reprimand, suspension, demotion, removal (dismissal), and criminal and civil penalties.

Continuous Monitoring. All users and devices, including governmental, commercial, grantee, and personal, connected to the Polar Science information infrastructure are subject to continuous monitoring for quality of service (QoS), security, vulnerabilities, attacks, threats, risks, and violations of these Rules of Behavior. Users are required to work with their IT point of contact (POC) to remediate weaknesses in their systems in a timely manner to reduce the risks to the Polar Science environment. USCG Management may rate limit, segregate, block, or disconnect without notice any user or device that poses an unacceptable threat or risk to the Polar Science network.

Acknowledgement. Your acknowledgement of these Rules of Behavior and your continued use of the system constitute your acceptance of these Rules of Behavior and of other relevant rules and regulations of the federal government and the U.S. Coast Guard. Acknowledgement is accomplished by signing a copy of this document as part of your account processing.

Questions. If you have any questions about these Rules, please contact the Polar Science Network Administrator. The responsible USCG point of contact for these Rules of Behavior is the Polar Science Branch Chief, Electronic Systems Support Unit, Polar Science Systems, 1519 Alaskan Way South, Seattle, Washington, 98134, 206.217.6552.

3. GUIDING PRINCIPLES FOR THE USE OF POLAR SCIENCE INFORMATION RESOURCES

In establishing these Rules of Behavior, the USCG has applied these guiding principles:

- The primary purpose of the Polar Science Network is to support science missions, so priority is given to scientific data and other work-related use.
- Polar Science information resources, especially aboard the research vessels, may be used for certain personal uses, in a manner that does not interfere with the program's mission. All mission activities take precedence over personal activities at all times.
- Personal communications, such as email or phone calls, that do not involve Polar Science business, will be considered entrusted communications, and not normally monitored or shared without the consent of the participating parties. Exceptions to this principle include requirements to make such communications available to support lawful investigations, to ensure proper operations and maintenance of the Polar Science infrastructure, or to correct or prevent damage to the Polar Science information infrastructure.
- Systems and network administrators, and others who may be exposed to a participant's personal communications as a part of their normal duties, are in a position of trust and will be held accountable for violations of that trust on their part.
- The U.S. Coast Guard is not a common carrier, and does not possess the requisite infrastructure and resources necessary to guarantee the privacy of information processed or stored on Polar Science information systems or networks. Users of Polar Science systems agree that the government and its representatives are not responsible for the loss of personal information, or for the disclosure

of personal information as a result of unauthorized activity by participants or by others outside the program.

Participants are expected to use good judgment in appropriate use of program assets consistent with the purposes of these Rules. However, the final determination regarding what constitutes appropriate use consistent with these Rules is assigned to USCG network management in coordination with the participant's organization.

4. NO EXPECTATION OF PRIVACY WHILE USING POLAR SCIENCE INFORMATION RESOURCES

Users of Polar Science information resources have no expectation of privacy with respect to any information residing on government information systems or transmitted over government information networks, other than the regular expectations associated with information governed by the Privacy Act of 1974, as amended. The USCG considers user information placed on Polar Science information systems or transmitted across the Polar Science information infrastructure to be entrusted information, which is not normally released for public viewing without the user's authorization. The USCG will release user information found on Polar Science information resources to appropriate law enforcement, or the Polar Science Information Security Team as part of an official investigation or other sanctioned activity. The USCG will, to the best of its ability, protect information within the Polar Science information infrastructure from unauthorized access. However, users make use of the government's information resources at their own risk. The USCG is not liable to the user for damages caused by unauthorized uses of the Polar Science infrastructure. Systems and Network administrators are authorized to access information located on Polar Science information resources or transmitted across the Polar Science information infrastructure when conducting their official duties. If such access occurs, the information will not be released for public viewing or to unauthorized persons.

5. ACCEPTABLE USES OF POLAR SCIENCE INFORMATION RESOURCES

The following activities are considered acceptable uses of the Polar Science Information Infrastructure. All users are reminded that Polar Science mission activities always take precedence over any personal activity. The USCG reserves the right to restrict or otherwise limit personal use based on resource availability, conflict with official business, and unacceptable information security risks.

Personal Use of Electronic Mail. Some limited personal use of the government's electronic mail services is permitted, provided it does not interfere with the participant's work or the work of others. Typical authorized limited personal use of email includes emergency communications and personal communications with family members, health care professionals, or teachers.

Personal Use of the Internet. Some limited personal use of Internet services is permitted, provided it does not interfere with the participant's work or the work of others. Extreme care must be taken regarding content matter. Typical authorized limited personal Internet use includes:

- Accessing travel information or forms on the or Internet
- Accessing parent organization information and online resources
- Accessing state and local government agencies on personal matters etc.
- Work-related events, such as technical symposiums, classes, and presentations
- Activities sponsored by the program, such as unit recreational activities
- Events and activities specific to a particular Polar Science unit or organization

- Program-sanctioned activities, such as blood drives, sanctioned clubs, and organizations
- Recreational web-browsing of a reasonable duration, during off-duty hours, that does not violate other elements of this policy and does not conflict with mission activities

Encryption of Personal Communications. Users may employ available encryption methods at their own expense on their non-Polar Science system when using the government's information infrastructure. Encrypted communications are still subject to monitoring and other authorized auditing actions. As a condition of use, users may be required to surrender their encryption key to appropriate USCG or law enforcement or the Polar Science Information Security Team to assist in authorized investigative activities.

Third Party Software, Freeware and Shareware. Users may not install third party software, including freeware and shareware on Polar Science systems.

Election Material. It is acceptable to use the Polar Science information infrastructure to disseminate information regarding the process to participate in U.S. federal, state and local elections. For example, information about absentee ballot procedures is allowed. Information advocating a position for or against a candidate, an issue, or other element of an election is not allowed.

Personal Business or Commercial Uses. While deployed, users may conduct limited business matters using government information resources, such as when a sub-contractor needs to communicate with their home organization .

Web Cameras and Collaborative Computing. Web cameras for training, meetings, educational outreach programs, or official business is permitted according to USCG policy and with the prior approval of the USCG.

6. PROHIBITED USES OF POLAR SCIENCE INFORMATION RESOURCES The following activities are prohibited uses of the Polar Science Information Infrastructure.

Illegal Activities. All illegal activities are forbidden.

Adverse Activities. Any activity that could embarrass the USCG, adversely affect its interests, interfere with the performance of the Polar Science mission, or exceed allocated resources is prohibited.

No Processing of Classified Information. The storage, processing or transmission of government classified information on unclassified computer systems, networks or via the Intranet and Internet is prohibited. All Polar Science information resources are to be considered unclassified and are not accredited for processing or transmitting classified information.

Hostile Environment. Under no circumstances is it permissible to access or download material that would create a hostile or offensive work environment, such as racist or sexually explicit material. This prohibition includes, but is not limited to, the following activities: accessing or transmitting sexual images, messages, jokes or cartoons; hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, age, national origin, or sexual orientation or is otherwise defamatory or derogatory; content prohibited by law and/or regulation.

Prohibited Email Activities. Allowing others to use an assigned email account is prohibited. Placing others on a mailing list, subscription list, chat room list, or other list service without their consent is prohibited. Creating, originating, distributing or circulating “chain” or “pyramid” transmissions, mass mailings, hoaxes, or harassing messages is prohibited. "All employee" or broadcast messages disseminated using Polar Science information resources must be business related and approved in advance by the applicable manager. Using large distribution lists for non-business-related purposes, or sending large, memory intensive files or applications which may impede or disturb network operation is prohibited. Using email to proselytize or solicit for personal commercial ventures, religious or political causes, or outside organizations is prohibited.

Personal Information Services. Due to resource constraints, personal servers of any type are prohibited. In the case of approved Science activities, all web services, file transfer services, and telnet/SSH services required for project support must be listed in the support requirements section of the user’s Science proposal and approved by the USCG.

Representation of Identity Online. The use of Polar Science information resources that result in user identity displayed or documented as affiliated with the Polar Science program (e.g., electronic mail addresses, IP network addresses, Polar Science.net domain name) produce the appearance of an official communication representing the U.S. Coast Guard. Only official use is sanctioned. Unauthorized use may be subject to administrative, civil, or criminal penalties

Mobile Code. The importation or use of unsigned mobile code is prohibited without prior written approval of the Polar Science Information Security Manager.

Streaming Media, Peer-to-Peer, and Gaming. Use of Polar Science information resources to participate in gaming, peer to peer networking, or streaming media usage activities is prohibited.

Prohibited Business and Commercial Uses. Conducting non-program business activities is prohibited. Using Polar Science resources to advertise commercial goods or services for sale for monetary or personal gain is prohibited. Using Polar Science resources to conduct non-program commercial activities is prohibited. Users may not establish or maintain a web-based business at a Polar Science operating location.

Prohibited Network Activities. Knowingly downloading, installing, storing or using malicious software, viruses, “cracking,” keystroke monitoring software or other actions that may be disruptive or counter-productive to business operations is prohibited. The introduction or use of packet sniffing software or any software intended to capture passwords is prohibited except when explicitly authorized for contract or business purposes and coordinated in advance with the USCG. Monitoring network traffic (e.g., running a sniffer); accessing IT resources; or copying data, files, or software without prior authorization is prohibited.

Wireless. The local Information Technology (IT) department regulates and manages access to wireless access points for connecting to the Polar Science network. Requests for access must be made to IT staff. The USCG also manages the radio frequency (RF) space in Polar Science operating locations. Unauthorized devices, whether connected to the Polar Science network or not, may be disconnected or blocked without notice. Users should be aware that a greater level of insecurity exists on a wireless network, and therefore assume that data transmitted over the wireless

network may not be secure, and take appropriate precautions. Exceptions may be considered if additional security controls are in place, and the request is approved in advance by the Polar Science Program Information Security Manager (Polar Science ISM).

Exceptions. Certain activities otherwise prohibited may be allowed in the performance of system administration or in other situations on a case-by-case basis at the discretion of the on-board technician. Exceptions may be made with bandwidth management in mind; under no circumstances will illegal activity or that which violates the security of the network be allowed.

7. ADDITIONAL GUIDANCE FOR USERS

User Responsibilities. When using the Polar Science information infrastructure you will be held accountable for your actions related to the information resources entrusted to you. Polar Science information resource users have the following responsibilities:

- Comply with these Rules of Behavior and all other Polar Science and USCG policies and procedures, as well as the policies and procedures of their sponsoring organization
- Protect sensitive information from disclosure to unauthorized individuals or groups. Disclosure of information is not at the users discretion, only when authorized by the USCG
- Ensure information security through effective use of user IDs and passwords
- Protect hardware, software, and information from damage, abuse, and unauthorized use
- Report security violations and vulnerabilities to the proper authorities. The ESU technician is the first point of contact for all reports
- Users shall not access, modify, duplicate, destroy, or disclose any information or software on a network or a computing system, unless so authorized
- Users shall not share their logon credentials with any other person.
- Users shall not leave an active system unattended, thereby allowing an unauthorized person to gain access to a network or a computing system through the user's login session
- Users are responsible to ensure the integrity, availability, and confidentiality of all work-related data on systems assigned for their use. It is recommended that critical data on a hard disk be backed up periodically. Data saved to the local workstation drives is not backed up by IT staff.

Authorization for Access. Portions of the Polar Science information infrastructure are restricted to authorized users who have been granted special access permissions by the U.S. Coast Guard or its authorized delegates. These areas are identified by warnings posted at their entry point or by the system's interactive request for authentication. You shall access only those areas for which you have been granted authorization to access.

Copyright and Intellectual Property Issues. All users of Polar Science information resources must comply with U.S. and international laws regarding copyrights and other intellectual property. Users must comply with copyright licenses associated with the Polar Science information resource they are using. Users shall not make copies of licensed software for other computers, users or for personal use. The presentation or display of digital media such as software, pictures, literary works and songs must comply with existing laws.

Alternative Workplace. When working at home or an alternative workplace, Polar Science information resources users must establish security standards at their alternate workplace sufficient to protect hardware, software, and information. This includes having only those resources employees really need and have authority to use; establishing a thorough understanding and agreement with supervisors as to what employees' security responsibilities are; using software

according to licensing agreements; ensuring that sensitive information downloaded is secure; being alert for anomalies and vulnerabilities; and reporting these anomalies to proper officials and seeking advice when necessary.

Personal File Storage. Each user is typically assigned a ‘home’ directory on their primary network which is usually accessible from any computer. This drive is provided for the storage of personal files. Files stored in this directory are not considered private, but will be afforded some measure of confidentiality against unauthorized access and disclosure.

Common File Storage. At each operating location, one or more directories are established for common use, and are accessible to all users. A temporary directory is provided for temporary (less than one week) use by users. Users have full rights to this directory and may add or delete files and directories as needed. All files and directories in the temporary directory are deleted automatically once a month, on a schedule determined by the station IT staff. A permanent common area is intended for operational storage and use. Users typically have read-only rights to this directory.

Departmental File Storage. Within each unit network, directories may be established for the various functional departments and participant organizations. Management of the allocated space is the responsibility of that department, with the assistance of the ESU technician. User privileges for their department directories are set at the discretion and with the approval of the department manager.

Equipment on the Polar Science Network. All equipment on the network is subject to vulnerability scanning. Polar Science participants are responsible for remediating vulnerabilities detected on their equipment. All equipment connected to the network, including server, laptops and other portable computing devices must be evaluated for compatible software and up-to-date anti-virus protection before they are used on the Polar Science network.

Official Business. Official business broadly includes any information processing that is required as part of an individual’s work responsibilities. Official business includes, but is not limited to, the performance of Polar Science work-related duties in position descriptions, professional training and class work, work covered under grant agreements with the USCG, tasks directed via USCG contracts, agreements with international partners, and support activities related to USCG contract tasking.

Ownership of Information. All information located on a government information system is the property of the government, unless otherwise identified as belonging to another entity as a result of a contract or a grant agreement with the government.

Personal Use. Personal use broadly includes any information processing that is conducted in support of activities that do not constitute official business. A personal use activity is typically one in which the individual user, or a non-Polar Science entity is the primary beneficiary. Participants who use program assets for personal purposes are responsible for any and all liability that may arise from such personal use to include any violation of law, regulation or policy during such use.

Use of Antivirus Applications. All users of Polar Science information resources must also comply with Polar Science policies regarding the use of antivirus software. Windows users must have antivirus software with signatures current to within two weeks of sailing or embarkation date.

Sensitive Information. The Polar Science information infrastructure can be publicly accessed. As such sensitive information must be properly handled. Sensitive information includes: medical, acquisition, operational security, proprietary, information security, and privacy data. Polar Science information resource users must acquire and use sensitive information only in accordance with established policies and procedures. This includes properly safeguarding sensitive information contained in hardcopy or softcopy; ensuring only those with a need to know have access, and ensuring sensitive information is accurate, timely, complete, and relevant for the purpose which it is collected, provided, and used.

Information Security. Access to the Polar Science Network or its corresponding network portals (i.e. Iridium, etc) may be restricted when ordered by the vessel's commanding officer or when the unit mission shifts to one of national security.

Reporting Violations. Users shall immediately report any known or suspected violations of these Rules or other Information Security policies or procedures. Please contact the Polar Science onboard Network Administrator at the e-mail address or extension listed in the welcome aboard brief.

8. ADDITIONAL GUIDANCE FOR CONTENT PROVIDERS AND SYSTEMS ADMINISTRATORS

Auditing of Information Systems. Information Technology, communications, and security personnel will regularly review telecommunications logs, text message logs, and conduct spot-checks to determine if users are complying with controls placed on the use of Polar Science information resources.

Protection of Personal Information. During the course of their duties, Content Providers and Systems Administrators may have access to information of a personal nature. This information is considered entrusted and is not to be disclosed unless authorized or directed to do so as part of a lawful investigation, or as directed by USCG management.