NSF Office of Polar Programs, Arctic Sciences Program

Information Security 101

April 2013

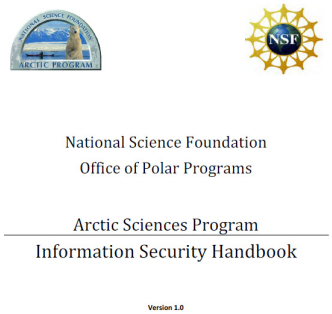
Issue 3

Special points of interest:

- **Avoiding unintended data loss or disclosure**
- **Handling and sharing personal information**
- **Google's policies and principles for users**

Inside this issue:

Introducing the Information Security Handbook


National Science Foundation
Office of Polar Programs

Arctic Sciences Program
Information Security Handbook

Version 1.0

The Arctic Sciences Section (ARC) Information Security Handbook provides policies specific to the ARC addressing Federal information security requirements and industry best practices. The handbook is intended for researchers, data managers, and other ARC participants.

The handbook reflects the primary focus of the ARC Information Security Program; to ensure confidentiality, integrity, and availability of Personally Identifiable Information (PII) and Sensitive Information (SI) managed by and on behalf of the ARC. The ARC Information Security Program also focuses on ensuring the security of systems essential for the operation of Arctic sites.

The first edition of the handbook provides guidance on:

- System security plans
- Security assessment and authorization
- Personnel security
- Physical and environmental protections
- Media protection
- Contingency planning
- Awareness training
- Incident response

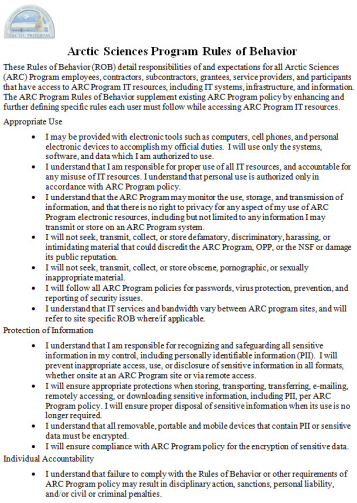
The handbook is available under *Information Security* on the NSF Arctic Research Support and Logistics web page.

Rules of Behavior

The ARC Rules of Behavior (ROB) details responsibilities of and expectations for all ARC Program employees, contractors, subcontractors, grantees, service providers, and participants who have access to ARC Program IT resources, including systems, infrastructure, and information.

The ROB informs all users of their responsibilities and expected behavior with regard to information and information system usage. Topics covered by the ROB include appropriate use of IT resources, requirements for protecting information managed on behalf of the ARC, and individual accountability.

The ROB is available under *Information Security* on the NSF Arctic Research Support and Logistics web page.


Arctic Sciences Program Rules of Behavior

These Rules of Behavior (ROB) detail responsibilities of and expectations for all Arctic Sciences (ARC) Program employees, contractors, subcontractors, grantees, service providers, and participants that have access to ARC Program IT resources, including IT systems, infrastructure, and information. The ARC Program Rules of Behavior supplement existing ARC Program policy by enhancing and further defining specific rules each user must follow while accessing ARC Program IT resources.

Appropriate Use

- I may be provided with electronic tools such as computers, cell phones, and personal electronic devices to accomplish my official duties. I will use only the systems, software, and data which I am authorized to use.
- I understand that I am responsible for proper use of all IT resources, and accountable for any misuse of IT resources. I understand that personal use is authorized only in accordance with ARC Program policy.
- I understand that the ARC Program may monitor the use, storage, and transmission of information, and that there is no right to privacy for any aspect of my use of ARC Program electronic resources, including but not limited to any information I may transmit or store on an ARC Program system.
- I will not seek, transmit, collect, or store defamatory, discriminatory, harassing, or intimidating material that could discredit the ARC Program, OPP, or the NSF or damage its public reputation.
- I will not seek, transmit, collect, or store obscene, pornographic, or sexually inappropriate material.
- I will follow all ARC Program policies for passwords, virus protection, prevention, and reporting of security issues.
- I understand that IT services and bandwidth vary between ARC program sites, and will refer to site specific ROB where if applicable.

Protection of Information

- I understand that I am responsible for recognizing and safeguarding all sensitive information in my control, including personally identifiable information (PII). I will prevent inappropriate access, use, or disclosure of sensitive information in all formats, whether onsite at an ARC Program site or via remote access.
- I will ensure appropriate protections when storing, transporting, transferring, e-mailing, remotely accessing, or downloading sensitive information, including PII, per ARC Program policy. I will ensure proper disposal of sensitive information when its use is no longer required.
- I understand that all removable, portable and mobile devices that contain PII or sensitive data must be encrypted.
- I will ensure compliance with ARC Program policy for the encryption of sensitive data.

Individual Accountability

- I understand that failure to comply with the Rules of Behavior or other requirements of ARC Program policy may result in disciplinary action, sanctions, personal liability, and/or civil or criminal penalties.

GoogleDocs and Cloud Computing

Google Docs and other cloud-based solutions for document sharing and management, such as DropBox, SkyDrive, Amazon Web services, or Terremark are frequently leveraged for business and personal use.

Many cloud-based solutions including Google Drive applications offer additional security services that can be purchased, such as back ups and customer support. The key is to understand the features available to you and plan your document management strategy before moving to the Cloud.

Users of cloud-based solutions need to be aware of the potential risks posed by using these tools before posting documents to these sites.

- Google accounts are often the subject of foreign attacks and a frequent target of malicious individuals. If a Google account is compromised, so are the documents that account has access to.
- General use of Google Docs does not include a service level agreement (SLA). If an SLA with Google is not in place the service may at times be unavailable without customer support, and there is no requirement for Google to return service within a guaranteed time frame.
- If you do not perform any formal/organized backups of data stored on Google Docs and are solely relying on Google you are risking losing your data as Google does not guarantee that your files will be maintained.
- If files are local you control who has access. With Google Docs, managing settings for access to files is more complicated. So, if you needed to terminate access for an individual to your Google Docs environment there is a risk that if the right settings are not implemented immediately your documents may be at risk.
- Based on Google terms and conditions they have full right to any document you place on Google Drive.

Encryption Option
If you must use Google Docs consider encrypting the Google Drive and sharing the key with users, which will protect your data from an attacker in the event of a breach.

Notes on Google's Policies and Principles for Users:

- Not all services are encrypted using SSL
- There are options for two step verification for accessing a Google Account, and a Safe Browsing feature available in Google Chrome *(however the two-step verification is optional and the Safe Browsing is provided by a third-party browser)*
- Information collection, storage and processing practices to guard against unauthorized access to systems are reviewed *(however these reviews have no defined standards or frequency criteria)*
- Access to personal information is restricted to Google employees, contractors and agents on a need to know basis, and are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

Important: When managing NSF data, remember that by default GoogleDocs is not compliant with the Federal Information Security Management Act (FISMA) and therefore cannot be used to manage documents containing Federal Agency information.

More Information on Google Docs Security Issues

http://techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs-without-permission/

Information Assurance Working Group

The Information Assurance Working Group (IAWG) is now established to include the Arctic research community and IT providers in the development of Arctic Information Assurance (IA) strategies. This IAWG hosted by SPAWAR, is comprised of 16 individuals representing key IT service providers supported by the Arctic Sciences Section.

The goal of the IAWG is to collaboratively discuss planned IT infrastructure and relevant Information Assurance/Security strategies to address vulnerabilities that reduce overall Arctic Program risk. The group will provide vital input to ensure that Information Security efforts being implemented are tailored to Arctic operational program needs, and that processes, policies and procedures are applied consistently, Arctic-wide.

IAWG Objectives:

- ◊ Facilitate open collaboration among Arctic IT stakeholders
- ◊ Ensure ARC security policies are operationally tailored
- ◊ Plan ahead for projects & science with IT impacts/needs, recommend solutions for ARC IT needs
- ◊ Create a vision and strategy for Arctic IT
- ◊ Address Federal and NSF security requirements
- ◊ Celebrate and share successes

Keep a look out for IAWG initiatives as they are highlighted in future newsletters.

SPAWAR Systems Center ATLANTIC

Social Media and Cyber Attacks

Social media technologies such as Wikis, blogs, and social networks (Facebook, LinkedIn MySpace, etc.) are vulnerable to spear phishing, social engineering, and web application attacks.

Spear Phishing targets a specific user(s) and attempts to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link. To convince the user to trust the phishing attempt, the attacker may use personal information about the target, such as places, events, and interests posted on a social networking site.

Social Engineering relies on exploiting trust by collecting information about the target, often available through Internet searches and on social networking sites. For example resumes, marital status, home address, phone numbers, employment information, work locations, family members, education, photos, etc.

Web Application Attacks exploit users by leveraging the dynamic tools often used by social networking sites, such as dynamic, interactive web pages that use scripting to provide additional functionality to the user. The extensive use of advanced web applications on social networking sites exposes the site and users to more exploitable vulnerabilities. For example, many applications available on Facebook are created by independent developers who often develop applications without considering security.

What To Do

Safe use of social media is based on user behavior, not technology, which makes it critical to make a conscious effort to protect data in all circumstances. Follow these guidelines to avoid inadvertently divulging sensitive information through a social network.

- Pay close attention to what information you plan to share, who you are sharing it with, and what information should not be shared
- Confirm the identity of people you don't know, before you share sensitive information with them
- Never share Personally Identifiable Information (PII) or Sensitive Information (SI) you have access to that is managed on behalf of the Arctic Sciences Program
- Be sure to inquire with RSL Program Managers before sharing if you are unsure if information about the Arctic Program should be shared
- Abide by Arctic Sciences Program Rules of Behavior when using social media websites
- Be mindful of blurring your personal and professional life
- Be aware of how you identify yourself on social media websites
- Avoid material that could discredit the ARC Program, OPP, or the NSF, or damage its reputation
- Don't establish relationships with working groups or affiliations that may reveal sensitive information about your job responsibilities
- Be aware of common attacks that occur on social media sites, such as those described earlier in this article
- Use the privacy controls available on social media sites to protect your own privacy and the privacy of the ARC Program by managing your personal profile and any profile you use for work-related activities. This may also involve removing certain data fields, such as employer details, work location, resume, skill descriptions, or other professional and personal information
- Always pay close attention to the details of online agreements before accepting or clicking 'OK'. Be sure agreements do not openly grant access to your information, which may include private and sensitive information you do not intend to share publicly

Information Source: *Guidelines for Secure Use of Social Media by Federal Departments and Agencies*

Social Media and Data Disclosure: In the era of social media keep in mind that what you post online can be interpreted by others as representing the NSF Arctic Sciences Program, and the entity whom you work for. Some unintended consequences of using social media include:

⇒ *Data Loss Prevention:* provides an easy way for unregulated information to leave the environment.

⇒ *Unintentional Disclosure*: The apparent anonymity of the Internet often results in people being more open than they would be if sharing information in person.

⇒ *Reputation*: Slander, rumors, and bad data propagate on the Internet, even when the initial source is deleted.

⇒ *Data Aggregation*: Information gathering about one individual from a range of different social networking sites to build a complete picture of an individual, which can result in identity theft.

⇒ *Infection:* Technically complex sites make it easier for your machine and network to be infected with a virus.

Information Source: http://www.infosecurity-magazine.com/view/2503/social-networking-a-risk-to-information-security/

Arctic Sciences Program Information Security Support is provided by SPAWAR Office of Polar Programs

Jack Buchanan Program Manager, SPAWAR Office of Polar Programs (SOPP)
843.218.5583
jack.buchanan@navy.mil

Sarah Wolfe OPP Program Manager
843.743.7642
wolfe_sarah@bah.com

Heather Fiebing Arctic Information Security Lead
303.221.0396
fiebing_heather@bah.com

SPAWAR Systems Center ATLANTIC

Handling and Sharing Personal Information

In conducting online affairs we are often required to share our personally identifiable information (PII) with others. Some examples of PII include credit card numbers, bank routing numbers, social security number, passport number, drivers license, and even a combination of full name and birth date.

⇒ When sharing PII and in handling the PII of others be sure to manage information securely.

⇒ Only share PII with those who have a need to know. When documents containing PII need to be shared for other purposes, remove PII from the document before passing it on.

⇒ Encrypt emails and files containing PII before sending. Information sent in clear text over the Internet can be intercepted by others who should not have access to your information.

⇒ Verify the entity requesting the information before sharing. Companies rarely call or email to request PII, so rather than providing the information when requested, call/email a known point of contact at the company to validate the request and provide your information to a known source.

⇒ Understand what the PII is being used for by the recipient, and how it is being managed. Depending on the entity, you may want to inquire about how they collect, use, share, safeguard, maintain, and dispose of PII.

⇒ If you work with PII managed by the Arctic Program, be sure to notify Arctic Science Program RSL Program Management if you think that Arctic managed PII may have been released (intentionally or unintentionally) to someone who does not have a need to know.

Arctic Management of PII and SI

To facilitate field support and travel for NSF-funded science in Arctic regions, the ARC Research Support and Logistics (RSL) Program manages personally identifiable information (PII) and Sensitive Information (SI) of program participants. Data managers follow measures described in the Arctic Sciences Information Security Handbook to ensure secure handling of PII and SI by:

- Limiting and monitoring access to information
- Securely using, storing, transporting and disposing of media
- Protecting, maintaining, and backing up systems storing data
- Training personnel on secure data handling practices
- Routinely assessing operational procedures and systems for continuous improvement

Security assessments have confirmed the RSL Program isolates the management of PII to systems and applications designed for that purpose, and routinely practice encrypting files containing PII when such information must be attached to an email. Other highlights include strong security of the data center hosting ARSLS Program Applications which manage PII, and detailed procedures to ensure isolated management of medical information necessary for the remote Summit Station in Greenland.

If you have questions or recommendations for RSL Program management of PII/SI, please contact a member of the Arctic Information Security Team provided by SPAWAR Office of Polar Programs.

Incident Response

Computer security incidents can compromise data, networks, and PII, among other services. An effective incident response program establishes processes and tools for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. If you suspect a potential security incident has occurred immediately report information on the event to the system manager or ARC personnel.

The ARC is required to meet Federal incident reporting requirements by reporting suspected and confirmed incidents to NSF IT security authorities. The NSF is required to report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the *US-CERT Concept of Operations for Federal Cyber Security Incident Handling.*

Reporting a Suspected Breach of Personally Identifiable Information (PII)

All ARC participants are responsible for recognizing and safeguarding PII in the possession of the government and/or designated contractors and representatives, and preventing inappropriate access, use, or disclosure.

In the event of a suspected or confirmed breach of PII, **immediately** report the incident to a member of the Arctic Information Security Team provided by SPAWAR Office of Polar Programs or an NSF Arctic Sciences Program Manager.