IRTF
IT
Security
Awareness
Training

IRTF IT Policy and Procedures Training for Staff

Slides generated in 2016

Presented by Miranda Hawarden-Ogata (IT Manager)

Quick Glossary

- ‘IT’ is short for ‘Information Technology’, a term used to refer to a collection of computer systems, services, networks, and other resources as well as the data stored within the collection.
- ‘UH’ is short for ‘University of Hawai`i’, the organization to which all staff at the IRTF belong.
- ‘Desktop’ and ‘workstation’ refer to a free-standing computer that usually resides on or under a table, most likely in a staff office or lab area.
- ‘Server’ refers to a computer that provides services such as email, printing, file-sharing, etc., and is generally located in a computer rack in a more segregated area (servers can be quite noisy)
- ‘BYOD’ is short for ‘Bring Your Own Device’

UH IT Procedures and Training

- UH provides an online security training program that can be accessed via the Laulima system. All IRTF staff are required to complete this training program annually. The training program and instructions may be accessed here:
    - http://www.hawaii.edu/infosec/training.html
- UH also provides an area to assist employees with securing information to which they have access, including general data protection guidelines and further resources for securing mobile devices such as laptops, smartphones, or tablet devices.
    - http://www.hawaii.edu/infosec/facstaff.html
- Important policies for computer disposal and email practices, among others, are listed here:
    - http://www.hawaii.edu/askus/706
    - http://www.hawaii.edu/askus/718

UH Information Policy Resources

- UH Policy E2.214 Security and Protection of Sensitive Information details the UH policy regarding sensitive information and can be viewed here:
  - EP 2.214 Security and Protection of Sensitive Information
- The UH Policies and Compliance page lists the various UH policies governing the usage of UH computer systems, networks, and resources. Also listed are the Hawaii Revised Statutes and other external regulations that apply to the resources provided by the UH.
  - http://www.hawaii.edu/infosec/policies.html
- UH Policy E2.210 Use and Management of Information Technology Resources Policy describes the appropriate use and management of UH IT resources and is the basis for university-wide policies and practices.
  - EP 2.210 Use and Management of Information Technology Resources

Copyright Material

- UH maintains a DMCA policy that can be viewed here:
  - http://www.hawaii.edu/askus/815

- All UH networks are covered by this policy, which includes all activity at Hale Pohaku, at any summit facility, and the IfA offices in Hilo, Manoa, and Maui.

IRTF Access Policy

- IRTF IT systems may be accessed via two methods:
  - Physical access
  - Electronic access
- Physical access is controlled by IRTF staff
  - IRTF IT systems are located in secure areas
  - Onsite staff maintain the security of those areas
  - Non-IRTF staff are only permitted supervised access
  - It is the responsibility of IRTF staff to maintain the physical security of the IRTF IT systems, such as keeping doors closed and/or locked when entering or leaving secure areas.
- Electronic access is available to both IRTF staff and observers who are not IRTF staff

IRTF Electronic Access

- Observer electronic access covers:
  - vnc access to the instrument interfaces
  - ssh access for transferal of macros and other observationally necessary files to guest accounts
  - sftp, rsync, scp allowing observing data to be downloaded
  - access to all public documentation on the IRTF website
- Staff electronic access covers:
  - ssh, sftp, rsync, scp (command line access)
  - vnc access to instrument interfaces and staff desktop computers
  - public and internal areas of the IRTF website
  - samba access to user account home directories and shared areas

Passwords “Best Practices”

- For more information about password best practices, take a look at the following sites:
  - http://security.fnal.gov/UserGuide/password.htm (Fermilab)
  - http://www.symantec.com/connect/articles/simplest-security-guide-better-password-practices (Symantec)
  - https://itservices.uchicago.edu/page/good-password-practices (U. of Chicago)
  - http://its.psu.edu/be-safe/password-best-practices.html (Penn State)
- Don’t be fooled by the dates on some of the articles. Password security hasn’t actually changed much over the years, and usually boils down to the same basic points.
  - use strong passwords with a variety of characters
  - do not write down passwords, or if you must, do not keep the password and username together, and store in a secured location
  - do not share passwords with anyone: staff members, family, or others

IRTF Password Security

- Shared Unix passwords for project accounts on IRTF computers are changed annually
- Shared VNC session passwords for instrument or other project accounts are changed daily.
- Shared and individual root accounts on various IRTF computers are changed annually.
- The internal area of IRTF website known as irtf-only is changed annually.
- Staff account passwords are the responsibility of staff to change and to keep secure.

IRTF Device Management

- Staff desktops and mobile devices are considered BYOD and management is the responsibility of the owner
- IT assistance is available if requested
- UH provides free software to all staff for protecting their computers:
    - anti-virus (http://www.hawaii.edu/askus/1254)
    - anti-spyware (http://www.hawaii.edu/askus/670)
- UH also provides a guide to securing desktop computers, which contains some of the links above as well as further information and advice:
    - http://www.hawaii.edu/askus/593
- Additional information about laptop best practices is provided here:
    - http://www.hawaii.edu/askus/927
- And similar information for mobile devices can be found here:
    - smartphones (http://www.hawaii.edu/askus/1419)
    - ipads and tablets (http://www.hawaii.edu/askus/1420)

Data Backup

- User and project account home directories are backed up daily and written to tape monthly
- Home directories can be accessed from your desktop or laptop. Contact the IT manager to get this set up.
- There is a finite amount of storage available to staff at any given time based on the size of the server disk space. Courtesy to fellow staff members in keeping personal or project home directory sizes manageable is appreciated by the IT staff.
- For large volumes of data, alternate methods of backup can be deployed such as additional hard drives in a desktop, personal RAID, etc. Options should be discussed with the IT manager prior to ordering parts.

Media Sanitation

- The IRTF policy regarding media sanitation is very simple: wipe or destroy.
- Functional computers or devices that will be donated should have their hard drives or media:
  - formatted and an operating system installed
  - wiped via approved wipe software to remove all data
- Non-functional computers or devices should have their hard drives or media destroyed.
- There are many sites that describe appropriate disposal of computer equipment:
  - The UH media protection policy outlined on the UH ITS site (http://www.hawaii.edu/askus/706)
  - The UH disposal guidelines for unused computer equipment (http://www.hawaii.edu/askus/750)
  - NIST Special Publication 800-88 (Guidelines for Media Sanitization) (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf)
- Approved software for wiping donated/recycled disks
  - DBAN (http://en.wikipedia.org/wiki/Darik's_Boot_and_Nuke)
  - linux shred (https://wiki.archlinux.org/index.php/Securely_wipe_disk)

Incident Reporting

- All staff are required to report any suspected computer security incident to the IRTF IT manager and/or the IRTF Director for investigation.
- Reports should be made immediately upon discovering a security incident as time is of the essence to prevent harm to the IRTF systems from a malicious attacker.
- All security incidents are included in the monthly techgroup IT report and should be discussed at the techgroup meetings.

Forms

- Reminders:
  - Please sign the Record of Training document and return to the IT manager as proof that you have attended this required training session.
  - You must complete the UH Information Security Awareness Training online and provide a copy of the Gradebook screen to the IT manager as proof of completion.
- Both documents will be kept on file as proof of training, and may be provided to external agencies in the event of an audit or as required by the UH or another government agency.