DRAFT

Wildland Fire Information and Technology Program Board
Incident Technology Support Subcommittee

Security White Paper #001

Incident Computer Security Procedures

Version 2.0

June 30, 2016

Purpose: This white paper is being published by the Incident Technology Support Subcommittee (ITSS) to provide a minimal best practices security policy that should be implemented in support of an Incident Management Team (IMT) responding to a Fire or All-Hazard Incident.

1. **Ensure that anti-virus software is installed, running and that definition files are current.**
   No computer shall be placed on the Incident network that does not have an anti-virus application installed and functioning properly. Prior to use of any computer on the Incident, each computer shall be checked to see if the anti-virus software package that is installed has current definition files and is updating automatically. This includes any computer that will be hooked up to the Incident network, regardless of ownership.

2. **The automatic update feature shall be enabled ensuring that critical updates are applied to the operating system.** The service may be disabled by the incident ITSS to limit excessive bandwidth usage; however critical updates must be applied manually. All current operating system critical updates shall be applied by their home office prior to each deployment.

3. **All users must sign an authorized Computer User's Acceptable Use Agreement.**
   This form shall be used to ensure that each user knows their responsibility as a user of the Incident system. Team members only need to sign once and copies of the signed form may be kept by the team's geographical area. Forms collected on an Incident will be filed in the Incident documentation box. (One version is attached as Appendix A. Agency specific forms may also be submitted.)

4. **Create unique usernames and passwords for all users.**
   If there is no other standard that a team uses, usernames should be in the form of first initial last name (e.g. *jdoe*) to better identify the user. All passwords must be at least 12 characters in length and need to include at least 1 each of the following types of characters: lower case, uppercase, number (0 – 9), and special character (i.e. !$#,%). Passwords must NEVER be shared.

5. **Implement password protecting, locking screensavers.**
   A locking screen saver shall be enabled on all computers at all times. No more than 15 minutes of inactivity shall elapse before the screen saver engages. The screensaver shall require a password to resume operations. The master database server will be configured with a locking screensaver after 5 minutes of inactivity.

6. **Provide role-based least privilege access to E-ISuite.**
   User accounts should only be assigned the minimum system roles necessary for the performance of specified tasks. Critical E-ISuite support and processing functions are distributed among different individuals or positions to ensure that no one person or position has all the authority or access necessary to conduct fraudulent activity or

compromise information security controls. Separation of duties in E-ISuite is primarily enforced by having separate user accounts for escalated roles/privileges such as Account Manager and Administrator.

7. **Document account access.**
   All requests for the establishment, modification or deactivation of user accounts and/or access privileges in E-ISuite will be documented on a User Account/Access Request form or General Message Form (ICS-213). Incident Management Team permanent member account access can be documented by using the hardcopy ROSS (Resource Ordering and Status System) Resource Order which documents the team's mobilization. Database Administrators will maintain paper copies of the completed forms as long as specified by agency policy.

8. **Perform periodic account reviews.**
   Periodic audits of user accounts will be conducted at least once during an incident assignment. This audit will include reviewing user account documentation (User Account/Access Request or General Message forms) for currency/completeness and removing roles from or deactivating any accounts for demobilized resources.

9. **Provide for network security.**
   A hardware firewall shall be installed between the Incident network and the internet. If wireless networking is used, it shall be secured to ensure that the only access to the network is from authorized users.

10. **Provide for physical security of electronic equipment.**
    All data on a Federal incident by default is labeled Sensitive but Unclassified (SBU). Computers and other electronic equipment that contain said information (NAS, data servers, cameras, GPS units, etc.) shall have a responsible party assigned and should be physically secured by locating the unit in a locked room or anchored to the work surface.

11. **Account for all equipment.**
    Equipment logs shall be kept for all items. Minimally the following information should be included: item location, responsible party, and serial number (if the unit has one). During transition, all equipment shall be accounted for and the receiving party shall sign for the equipment being transferred.

12. **Personally owned equipment prohibited.**
    The Incident is not responsible for unauthorized computers brought to or used on the Incident. Only authorized computers (agency or incident provided) will be allowed to be connected to the Incident network.
    a. Reference Forest Service Policy: FSM 6161.31 and FSM 6683.15, paragraph 6
    b. Reference Department of Interior Policy: Department-wide Rules of Behavior for Computer Network Users, page 6, item 9.

13. Perform backups regularly.

Backing up the E-ISuite database and the Incident filing system is crucial. The E-ISuite database has an automatic backup feature which should be enabled and minimally, copies of this file should be moved to a separate computer or external drive on a daily basis. The database should be uploaded to the E-ISuite repository at each transition and incident end. A copy shall be given to the local administrative unit at the end of the Incident in accordance with the NWCG Data Repository Memo dated July 19, 2004. All other copies of the E-ISuite database must be destroyed or sanitized.

Copies of the Incident filing system must be safeguarded from theft. To that effect, it is important that copies of incident data are not handed out to team members. Some information that resides in the Incident filing system (i.e. Finance, Human Resources, and Medical) must be made available to only authorized individuals. The Incident filing system should be backed up daily. Should the backups be to portable media, the files must be encrypted.

14. Sanitize non-agency computers.

Because there is sensitive data and documents on the computers attached to the network, non-agency computers must be sanitized at the end of an Incident or prior to returning them to the vendor. Sanitizing a computer is the process "electronically shredding" the information stored on the hard drive such that the information is not recoverable. An alternative that is acceptable for team computers is the use of "file and folder shredders". These applications will sanitize individual files and folders in an operating system and can be automated to perform the wipe on a specified schedule.

15. Maintain control of external storage devices.

Make users aware of the rules of behavior as it relates to data. Incident data should not be stored on drives or devices that are not under the control of the Incident. Encryption must be used on external drives whenever possible.

16. How to handle digital images.

Pictures taken at an Incident by incident personnel using Government owned equipment belong to the host agency. These images must be treated as data and not be given out to individuals without prior approval from the appropriate managing entity. A policy should be developed by each team as to how to handle digital images, especially any sensitive photos.

17. Reporting loss of data or equipment.

Securing the network and safeguarding the data is the responsibility of the ITSS and the ITSS may be held liable for loss of equipment or data unless a team security policy exists and is followed. If there is a loss of sensitive data or equipment at an Incident the following steps must be taken:

- Inform Command and General Staff as well as the Security Manager (who will coordinate contact with Law Enforcement).
- Inform the agency to which the Incident is reporting so that they may activate their Computer Security Incident Response Team (CSIRT) if necessary.

- Notify the owner of the loss of the equipment.
- Provide for the continuity of operations for the Incident.
- Document all actions.

In situations where there has been a breach in security and it is suspected that personally identifiable information (PII) has been compromised, the United States Computer Emergency Readiness Team (US-CERT) must be contacted within one hour of discovery/detection. This reporting requirement does not distinguish between potential and confirmed breaches of PII or the form of data loss (i.e., physical or electronic) and is the responsibility of the hosting agency.

18. Team computer configuration.

Team computers should be configured so that they do not boot from a floppy, USB port or CD, only from the hard drive. Also, access to the BIOS should be password protected. The E-ISuite server should be similarly configured. Take care to document any passwords used on leased equipment. It is VERY important that BIOS passwords that are set during the Incident are cleared before returning the equipment to the leasing company at time of Demobilization.

Appendix A - Acceptable Use Agreement

Individual Computer User's Acceptable Use Agreement

GENERAL RULES AND GUIDELINES GOVERNING THE USE OF FIRE GENERAL SUPPORT SYSTEMS

Violations of the following rules are considered computer security incidents:

1. CLASSIFIED INFORMATION. Do not enter any classified National Security information into any Fire General Support System.

2. GOVERNMENT PROPERTY. Computer hardware, software, and data are considered to be the property of the U.S. Government. Fire computer systems are used for official business only. Do not use games, personal software, private data, unlicensed proprietary software, personal peripherals or otherwise non-government information or enter them into any Government-owned computer system. Any use of computers, software or data for other than official business is expressly prohibited, except as permitted by the Fire Teams Internet Acceptable Use Policy.

3. PROPRIETARY PROPERTY. Commercially developed and licensed software is treated as proprietary property of its developer. Title 17 of the U.S. Code states, "It is illegal to make or distribute copies of copyrighted material without authorization." The only exception is the user's right to make a backup for archival purposes, assuming one is not provided by the manufacturer. It is illegal to make copies of software for any other purpose without permission of the publisher. Unauthorized duplication of software is a Federal crime. Penalties include fines of up to $100,000 per infringement and jail terms of up to five years.

4. ACCOUNTABILITY. Individual User IDs and passwords are assigned only to persons having a valid requirement to access Fire General Support Systems and local/wide area networks. All activity accomplished under this User ID is directly attributable to the user to whom it is assigned.

GENERAL BUSINESS PRACTICES, if not followed, can lead to security incidents as listed below. Noncompliance with these practices may result in removal of access and/or disciplinary or legal action being taken, consistent with the nature and scope of such activity.

1. INDIVIDUAL USER IDs AND PASSWORDS. Do not share your individual User IDs and passwords. They are to be used only by the individual owner. Do not write down user IDs and passwords, except on the original assignment document. Destroy this document once memorized, or at a minimum, keep it in a safe place. Under no circumstances should User IDs and passwords be posted ANYWHERE! Do not keep them in accessible locations. Never use personal information (e.g., telephone numbers, names of family members, pets, etc.) or dictionary words for your passwords. Passwords must be at least eight characters in length and consist of at least one uppercase, one lowercase, one numeric character and one special character. Passwords are changed at required intervals. If you believe your User ID and password have been compromised, change your password, notify your supervisor, and report the incident to the Team ITSS.

2. UNAUTHORIZED ACCESS. Access to Fire computer systems requires management approval. Do not attempt to gain access to any Information Technology system for which you are not approved nor have authorization to access.

3. LOG OFF when not actively working on the computer system. At a minimum, lock your workstation when leaving your work area for short periods of time or invoke the computer system's locking screen saver. Remember, you are responsible for all activity logged under your User ID.

Individual Computer User's Acceptable Use Agreement

I, the undersigned, understand that when I use any of the Fire General Support Systems and/or applications or gain access to any information therein, such use or access is limited to official Government business. Further, I understand that any use of the aforementioned systems or information that is not official Government business may result in disciplinary action consistent with the nature and scope of such activity. I have read the "General Rules and Guidelines Governing the Use of Fire General Support Systems.". I understand and agree to comply with them.

☐ Federal Employee

_____
Agency / Organization

☐ Non-Federal

_____
Name of Organization / Company

☐ Contractor Employee

_____
Contract Company

☐ Administratively Determined (AD) Employee

_____
Agency / Organization

_____ _____
Individual's Typed or Printed Name Individual's Signature Date

USER: RETAIN GENERAL RULES AND GUIDELINES FOR YOUR RECORDS AND REFERENCE