

National Wildfire Coordinating Group
Information Resource Management Working Team
Computer Technical Specialist Task Group

Security White Paper #001

Incident Computer Security Procedures

Version 1.2

June 1, 2007

Purpose: This white paper is being published by the Computer Technical Specialist Task Group (CTSPTG) to provide a minimal best practices security policy that should be implemented in support of an Incident Management Team (IMT) that has responded to a Fire or All-Risk 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. All users must sign Individual 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 per season and copies of the signed form may be kept by the team's geographical region. Forms collected on an Incident will be filed in the Incident documentation box. (An Acceptable Use Agreement form is attached as Appendix A.)

3. Create unique usernames and passwords for all users.

Usernames should be in the form of first initial last name (e.g. *jdoe*). Passwords must be at least 8 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.

4. 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.

5. 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 insure that the only access to the network is from authorized users. Internet access should be granted on a case-by-case basis. For example: Situation Unit Leader, Cost Unit Leader, Finance Section Chief, Demob Unit Leader, GIS. Other security requirements may be identified. For more information on securing a wireless network see Security White Paper #002.

6. Provide for physical security of electronic equipment.

Computers and other electronic equipment that are deemed sensitive (snap servers, cameras, GPS units, etc) shall have a responsible party assigned and should be secured at all times. Make sure that equipment is not left unattended in high traffic areas.

7. 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 applicable). During transition, all equipment shall be accounted for and the receiving party shall sign for the equipment being transferred.

8. Personally owned equipment prohibited

The Incident is not responsible for unauthorized computers brought to or used on the Incident. Only authorized computers will be allowed to be connected to the Incident network.

9. Perform backups as needed

Backing up the I-Suite database and the Incident filing system is crucial. The I-Suite database has an automatic backup feature which should be enabled and minimally, copies of this file should be moved to a separate computer on a daily basis. The database should be uploaded to the I-Suite repository at each transition and a copy 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 I-Suite database must be destroyed or erased. Copies of the Incident filing system must be safeguarded from theft. To that effect, it is important that complete copies 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.

10. Sanitize non-agency computers.

Because there could be sensitive data or documents on any of the computers attached to the network, non-agency computers should be sanitized at the end of an Incident or when they are demobilized. Sanitizing a computer is the process of writing information to the hard drive such that the data stored on the hard drive is not recoverable. Also, team computers should be processed in a way that permanently removes sensitive information that may have resided on the equipment.

11. 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 should be used on external drives.

12. How to handle digital images.

Pictures taken at an Incident belong to the host agency. They should be treated as data and not be given out to individuals. A policy should be developed by each team as to how to handle digital images, especially any sensitive photos.

13. Loss of Data or equipment.

Securing the network and safe guarding the data is the responsibility of the CTSP and the CTSP may be held liable for lose 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 should be taken:

- Inform Command and General Staff and Security.
- Inform the agency to which the Incident is reporting.
- Notify the owner of the loss of the equipment.
- Provide for the continuity of operations for the Incident.
- Document all actions.

14. 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 I-Suite server should be similarly configured. Take care to document any passwords used on leased equipment. It is VERY important that passwords that are set during the Incident are cleared or turned over 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 CTSP.
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 do not have an approved and 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