Sensitive Information Management and Responsibilities

GEN502

January 2013

Managing Sensitive Information - Why

- To achieve its mission, Jefferson Lab uses Information Technology (IT) that stores and processes broad categories of Sensitive Information:
  - Business Sensitive
    - Financial, procurement, contracts, Intellectual Property (IP), proprietary, etc.
  - Personnel Sensitive
    - Personally Identifiable Information (PII), HIPAA (medical), salaries, appraisals, personnel records, etc.
  - Attorney-Client Privileged information
  - Science and Technology Sensitive
    - Export controlled (Department of Commerce and Department of State)
    - Access to Export Controlled Sensitive Information is not permitted to non-U.S. persons even if they are in the U.S.
      - *U.S. persons* include U.S. Citizens plus U.S. Lawful Permanent Residents, also known as "Green Card" holders.
  - DOE Official Use Only (OUO), DoD For Official Use Only (FOUO), Distribution Statements C, D, etc.

- ***Important: Jefferson Lab's government facility clearance is UNCLAS; classified national security information is not permitted on site.***

- The Jefferson Lab policies for handling Sensitive Information are online at:
  - https://cc.jlab.org/sensitiveinfo

Managing Sensitive Information - Why

- It is a best business practice to properly manage Jefferson Lab's Sensitive Information.
  - Decreases risks and liabilities.

- For several classes of Sensitive Information, proper management of the information is the law, required by federal codes, and/or the JSA contract with DOE. There may be significant civil and/or criminal penalties for both the individuals involved and JSA for mismanagement, intentional violations or mishandling of these classes of Sensitive Information.

Sensitive Information on IT Systems- Where

- Most Lab Sensitive Information on IT systems is on one of three enclaves (Jlab's IT systems are placed in 10 enclaves). These three enclaves have Federal Information Processing Standards (FIPS) 199 Moderate cyber security controls:
  - Business Admin
  - Core Systems (including central email, certain file systems and backups)
  - FEL

- In addition, scientists, engineers, administrators, etc. (staff and users) may have information on their IT systems that they are treating as sensitive. Examples include:
  - Pre publication data
  - Third party proprietary/confidential data which is protected by non-disclosure agreements
  - Intellectual property
  - Personnel actions

Sensitive Information Physical Security

- FIPS 199 Moderate controlled Core IT systems and media are in secured areas.

- Most Moderate controlled desktop systems are in lockable offices in designated areas.

- When you work in these areas you may see hard copy documents with Sensitive Information. All Sensitive Information controls apply to hard copy documents as well.

Sensitive Information Physical Security

- Each group typically has its own group specific Sensitive Information processes and procedures for both IT systems and hard copies.

- Staff are responsible for separately signing any group specific acknowledgements for working with Sensitive Information.

Sensitive Information – Roles and Responsibilities

- Line managers and individuals who create and use Sensitive Information are responsible for protecting it. They should create written procedures for the proper handling, control, and disposal of Sensitive Information they are responsible for to ensure it is protected in accordance with JLab policy.

- Records Management (Kim Kindrew, 7805) in the IT Division coordinates the procedures for retention and destruction of Sensitive Information that is considered to be records or vital records.

- Consult with JLab Cyber Security about methods of reusing IT equipment and media that contained Sensitive Information through the Computer Center Help Desk (7155).

- Contact JLab Property (Carl Iannacone, 5430) about disposing or excessing IT equipment and JLab Security (Kris Burrows, 7548) about properly destroying hard copy Sensitive Information or electronic media, CDs, memory sticks, hard disks, etc.

Awareness of IT System Sensitive Information

- Be vigilant when working on systems with Sensitive Information.
- Remember that there are many categories and sub-categories of Sensitive Information.
- Be situationally aware, i.e. pay attention to whether the system you are working may contain Sensitive Information.
- When in doubt, contact the CIO (Roy Whitney, 7536), the Head of CNI (Andy Kowalski, 6224) or the Cyber Security Manager (Greg Nowicki) for clarification.

Your Responsibilities

- As a staff member with administrative responsibilities or an IT system professional, you typically have access to hard copy Sensitive Information IT and/or IT systems at the network/systems admin/root/database level. You may also work with end users that are accessing Sensitive Information or you may happen to see Sensitive Information while working on the networks, servers, etc. or while working with hard copy sensitive information.

- Consequently, you are responsible for the proper handling and management of all Sensitive Information that you may encounter.
  - Do not discuss this information with anyone who does not have a legitimate business "need-to-know" and proper training.
  - Do not use this information for any personal gain, ex promotions, salary increase requests, etc.

- Failure to meet your responsibilities for Sensitive Information can result in Jefferson Lab administrative discipline and/or civil and/or criminal penalties.

What to do when there are problems

- If you discover an IT system, hard copy system and/or business activity with Sensitive Information and/or activities that are not being properly managed, immediately inform your supervisor. He/she will inform Security Manager (Kris Burrows, 7548), Cyber Security Manager (Greg Nowicki, 6105), Head of CNI (Andy Kowalski, 6224), HR Manager (Rhonda Barbosa, 5991) and/or CIO (Roy Whitney, 7536).

- If you disclose Sensitive Information (inadvertently, accidently, by intent, etc.) immediately inform your supervisor. He/she will inform the Security Manager, Cyber Security Manager, Head of CNI, HR Manager and/or CIO.

- You may also go directly to the Security Manger, Cyber Security Manager, Head of CNI, HR Manager, CIO, etc. as appropriate.

Summary

- Take Sensitive Information management seriously.
  - Both legal regulations and Jefferson Lab administrative requirements assess significant penalties for improper management, mishandling or intentional violations.
  - Our contract with DOE requires proper management, and the program offices (i.e. people sending us funding) expect that Sensitive Information is properly protected.
  - Proper handling and awareness of Sensitive Information requirements are part of your job expectations.

- Remember:
  - Employees may use Sensitive Information only in the conduct of JLab business
  - Employees may not use Sensitive Information for personal gain.

- Done well, management of Sensitive Information is a strength of the Lab and assists us in meeting long-term strategic goals for Jefferson Lab programs.

Sensitive Information Management and Responsibilities

- I understand the policies and procedures for management of Sensitive Information have been established for the protection of this information and that my failure to follow these policies and procedures may result in personnel actions as delineated in the Jefferson Lab Administrative Manual and/or civil and/or criminal penalties.
- I acknowledge and understand that Sensitive Information may be subject to U.S. Export Control Laws and Regulations from the Department of Commerce and/or Department of State and/or be part of JSA's contract requirements with DOE, and that an export license may be required to pass Sensitive Information to non-U.S. persons and/or entities. I also acknowledge and understand that should I inadvertently disclose or receive defense articles for which I have not been granted a license to disclose or access authorization by the U.S. Department of State, Directorate of Defense Trade Controls, I will report such unauthorized disclosures and acknowledge the transfer to be a violation of U.S. Government regulations.

Click on the button, and enter your information to complete this training and your certification.

Next