Security Plan for Protection of Sensitive Information

Thomas Jefferson National Accelerator Facility

I. Introduction

This Security Plan addresses the information security, physical security and cyber security requirements that govern Sensitive Information (including sensitive data) present at the Laboratory. The procedures in this Security Plan have been approved by the Laboratory Director and shall be adhered to by all Laboratory staff and users in the conduct of their work.

Appendix A of the CSPP, hereto, provides a listing of Enclave and Department security plans specifically tailored to supplement the requirements of this Security Plan (including annual certification requirements). In the event of a conflict between this Security Plan and specific Department requirements, the more stringent requirement shall be applicable.

II. Identifying Sensitive Information

A "document" as used in these procedures means recorded information or data regardless of its medium or characteristics (e.g., written reports, pictures, graphs, financial data, etc. or electronic documents stored on hard drives, floppy discs, tapes or being transmitted over networks.)

"Information" refers to the facts, data, or knowledge itself regardless of the medium of its conveyance, and therefore, documents are deemed to convey or contain information and are not considered to be information per se.

The Laboratory's DOE approved facility clearance does not authorize storage of Government national security information typically referred to as "Classified" information on site(e.g., CONFIDENTIAL, SECRET, or TOP SECRET which are federal agency security labels) In the event that you observe marked documents or equipment anywhere on Laboratory property immediately notify the JLab Facility Security Officer as soon as practical via the JLab Security Control Center or the Facility Management Administration desk.

Sensitive Information is to be categorized in one of the following classifications (section of this document):

- Business Sensitive (II.A)
- Personnel Sensitive (II.B)
- Attorney-Client Privileged (II.C)
- Official Use Only (OUO) (II.D)
- For Official Use Only (FOUO) (II.E)
- Unclassified Controlled Nuclear Information (UCNI) (II.F)
- Other

For information to be considered "Sensitive Information", the information must have the potential to damage Laboratory, governmental, commercial, or private interests if disseminated to persons who do not need the information to perform their jobs or other Laboratory/DOE-authorized activities. The possible consequences to such interests should be carefully considered in each case when confronted with potentially Sensitive Information. However, information that is available in the public domain is generally not Sensitive Information.

Following are the categories and examples of Sensitive Information in use at the Lab. General requirements for management of Sensitive Information are in sections III through VI.

A. Business Sensitive Information

The following provides examples of the potential types of Business Sensitive information found at the Laboratory: Note, this information may be the result of the Laboratories' own business activities, provided by a vendor, sub-contractor or funding agency, or a combination of these entities.

Commercial/proprietary information generally concerns information such as trade secrets, business plans, financial or cost data received from a company doing business or contemplating business with the Laboratory. Personal statements or documents supplied by contractors in the course of inspections, reviews, site visits, investigations, or audits when such information is received in confidence should also be maintained as business sensitive.

Information produced by JLab in the performance of work (basic research, Cooperative Research and Development Agreements, Work-for-Others agreements, etc.) may be considered proprietary by the Laboratory or vendor or subcontractor to the Laboratory and consequently be Business Sensitive Information. Also, privileged information such as Laboratory acquisition/evaluation plans, and results of evaluations and audits should be maintained as Business Sensitive Information.

Intellectual property, contract negotiation information, procurement data, patentable design bids, and research and development information considered proprietary are usually to be considered Business Sensitive Information. Pre-decisional information involving internal Laboratory business communications or plans that have not been published or determined to be final may be Business Sensitive Information.

Frequently, Business Sensitive Information often has a time limit, ex: procurement information prior to award and product performance characteristics prior to public announcements.

B. Personnel Sensitive Information

Personnel Sensitive Information includes personnel and medical files and similar files whose disclosure would constitute a clear unwarranted invasion of privacy. Examples include employee payroll data, tax reports and payments, payments for employee benefit and welfare plans, travel related costs and information, employee performance information and medical records. Note, this information usually falls under the protection of the Privacy Act of 1974. Personally Identifiable Information (PII) (see http://cc.jlab.org/services/security/ for PII policies and procedures) is Personnel Sensitive Information.

C. Attorney-Client Privileged Information

Attorney-client privileged information or working papers prepared by an attorney in contemplation of litigation. Contact JLab legal counsel for instructions before creating or accepting any information that may be considered "Attorney-Client Privileged Information.".

D. Official Use Only (OUO).

"Official Use Only" is an official designation used by elements of the Department of Energy to identify and control business sensitive documents. JLab staff should notify the CIO if they receive government marked OUO in the performance of their duties and should not create OUO without the prior approval of the CIO. Staff who have a duty and mission requirement to retain OUO documents or information shall contact the CIO for instructions on the management of these documents.

E. For Official Use Only (FOUO)

"For Official Use Only" is an official designation used by elements of the Department of Defense to identify and control business sensitive documents. JLab staff should notify the CIO when they

receive government marked FOUO in the performance of their duties and should not create FOUO without the prior approval of the CIO. Staff who have a duty and mission requirement to retain FOUO documents or information shall contact the CIO for instructions on the management of these documents.

F. Unclassified Controlled Nuclear Information (UCNI)

The U.S. Department of Energy and U.S. Department of Defense categorize certain unclassified information concerning the security of nuclear material use facilities or nuclear materials that could have a military application, regardless of its physical state or form. The unauthorized disclosure of this information may be useful to a malefactor in defeating part of a security system and result in an adverse effect, while not leading to damage to the national security. JLab staff shall notify the CIO when they receive government marked UCNI in the performance of their duties and shall not create UCNI marked documents without the prior approval of the CIO. Staff who have a duty and mission requirement to retain UCNI documents or information shall contact the CIO for instructions on the management of the documents.

G. Other

The Laboratory may receive Sensitive Information from various funding agencies, vendors, sub-contractors, etc. with other labels. Examples might include: Law Enforcement Sensitive, Export Controlled Information (ECI), Sensitive Unclassified Information (SUI), Foreign Government Information (FGI), Strictly Private Information (SPI), Naval Nuclear Propulsion Information (NNPI), etc. JLab staff shall not use any of these classifications for sensitive information without the prior approval of the CIO. Any staff creating or receiving documents or information with these categories shall contact the CIO for instructions on the management of these documents.

III. Marking Business Sensitive and Personnel Sensitive Documents

A document that is deemed sensitive according to Section II of this document should be clearly marked on each page to indicate the nature of its sensitivity, except that documents maintained in restricted files do not need to be marked while in these files or when retrieved from the files for reference, inventory, or similar purposes as long as the documents will be returned to the files and are not accessible by individuals who are not authorized to have access to the information. When marking sensitive documents the following designations should be used:

A. Business Sensitive
B. Business Sensitive- Attorney Working Papers
C. Personnel Sensitive
D. OUO, FOUO, UNCI, etc. shall not be used without prior permission and instructions from the CIO.

Documents that have been previously identified as “proprietary” or “official use only” are by their nature business sensitive, and no further marking of the document is necessary.

IV. Safeguarding Business Sensitive and Personnel Sensitive Data

JLab employees are responsible for the safekeeping of Sensitive Information under their control. Accordingly, the following precautions should be taken to protect Sensitive Information against release to unauthorized persons:

Physical Storage

Store documents and computer media in appropriate receptacles (Department groups should determine the level of protection required for specific documents, i.e., fire proof safes, locked files or desk drawers, etc.). Locking the office alone is not adequate.

Computer Lockout

If your computer contains Sensitive Information, it should either be turned off or have a screen saver that locks out access whenever you are not at your desk. Certain applications run by specific groups may have additional security requirements including secondary passwords or other security features beyond those provided by the central systems. Any such additional security requirements will be documented in that group's security plan.

File Permissions

File and directory permissions shall be configured to prevent "World Read" and in most cases "Group Read" of Sensitive Information. Staff can contact the Helpdesk for assistance in setting their file and directory permissions.

Portable Systems and Media

Security requirements/features for desktop/portable computers and removable media are discussed below (see Sections VII and VIII).

Locked Offices

Offices containing Sensitive Information shall be locked when vacated at the end of each workday.

Visitor Control

Staff should be vigilant to ensure that visitors (including contractors) cannot access Sensitive Information without authorization.

Networked Printers

Extreme caution should be exercised when printing sensitive documents using networked printers. An inadvertent compromise of protected information may occur if a document does not print immediately, may be retained in the print cue memory and print out at a later date and time when not expected.

V. Disclosure of Sensitive Data

Sensitive Information shall not be disclosed to individuals who do not have a business need to know. Sensitive data such as credit card numbers or social security numbers should be expunged on working documents (e.g. receipts, invoices, etc.) whenever possible.

Sensitive data of others will be managed in accordance with the terms of any negotiated non-disclosure agreements (NDAs) and at least with the same care applied to the management of Lab Sensitive Data.

When sending sensitive information by mail place it in a sealed, opaque envelope and write "Business Sensitive" (or Personnel Sensitive) "To Be Opened By Addressee Only" on the outside.

VI. Retention and Destruction of Sensitive Information

Laboratory staff should periodically review all assigned files and documentation and destroy/shred extra (duplicate) copies that are no longer needed using a JLab approved shredder. Original copies of sensitive records should be retained through the required retention period for such documents and then released to the JLab Record Custodian for destruction.

Obsolete or duplicate computer disks and other removable media containing Sensitive Information should be hand carried to Facility Management Administration for disposal in the bulk shredding collection container.

VII. Electronic Security

For sensitive information in and on electronic media, security is vital in maintaining confidentiality of data as well as protecting the integrity of our financial systems and our business processes. The cyber security aspects of dealing with electronic sensitive information are included in the Lab's Cyber Protection Program Plan (CSPP). In this plan, computer information security (cyber security) is addressed through a cooperative effort involving the JLab Information Technology Division and line managers of those divisions, departments and/or groups with

Sensitive Information. Note, the next revision of this policy will include encryption requirements for sensitive information.

VIII. Jefferson Lab Cyber Security Architecture

The CSPP provides the site wide cyber security architecture along with requirements for managing information in the cyber format. As part of the cyber security aspects of the site cyber infrastructure, the cyber systems are divided into a number of enclaves. Those enclaves with high concentrations of Sensitive Information have enclave specific cyber security plans. Some elements of these plans are associated with specific work groups.

IX. Promulgation of Procedures

The Lab's computing community shall be made aware of the policies formulated in this document by means of:

A. The computer user agreement that is signed by all people requesting a new computer account,
B. specific guidance presented in the annual security awareness training,
C. confidentiality agreements signed by staff who work in enclaves that contain sensitive information, and
D. guidance and confidentiality agreements issued by the CIO and signed by managers and administrative staff who may handle Sensitive Information.

X. Determining Sensitive Information

All divisions, departments and groups are responsible to collaborate with the CIO and the Lab Security Manager on determining if information or data in their purview is Sensitive Information. If sensitive property is also involved, this shall be part of the collaboration. The management procedures for the Sensitive Information and Sensitive Property shall be included in the appropriate group security plans.