Jefferson Lab
Thomas Jefferson National Accelerator Facility

JSA
A SURA Company

CONFIDENTIALITY AGREEMENT

Compliance with and effective enforcement of the Code of Ethics and Standards of Conduct is an expectation of all employees. As part of my job duties at Jefferson Lab, I will have access to data considered to be private personnel data *and/or* business sensitive *and/or* Personally Identifiable Information (PII) to JSA/Jefferson Lab.

I agree that I

- Will not disclose any information to which I am privileged to parties that do not have a business need,
- Will not use any knowledge I gain to the detriment of any person or any Lab activity,
- Will not use any knowledge I gain for personal benefit,
- Will not seek out, access, or view personnel sensitive, business sensitive, or personally identifiable information without an explicit business need to do so required to perform my job function,
- Am responsible for safeguarding all sensitive information and will properly mark, store and transmit it in accordance to guidance. If I need assistance identifying whether information is sensitive, I will seek guidance from the Security Office at fso@jlab.org or Cyber Security Office at helpdesk@jlab.org,
- Understand Personally Identifiable Information should only be handled by those with a need and shall not be held on memory sticks or other portable memory devices without explicit permission from the Laboratory,
- Will report any suspicion of PII compromise to the Lab within 5 minutes. This includes non-business working hours such as nights and weekends. Suspected compromise should be reported by calling the security guards at 757.269.5822.

The handling of private personnel data or information is in keeping with the Lab's Code of Ethics and Standards of Conduct which state:

- Each of us must conduct all aspects of JLab business in an ethical and lawful manner.
- Each of us must hold ourselves to the high standards of honesty, integrity, and fairness in relationship to others.
- Committing acts that may constitute unethical behavior or create an organizational conflict of interest is considered inappropriate conduct.

DEFINITIONS

Depending on my role, I recognize and understand I may have access to some or all of the following:

Personnel Sensitive Information is information if lost, compromised, or disclosed could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual including personnel and medical files and similar files whose disclosure would constitute a clear unwarranted invasion of privacy. Note, this information usually falls under the protection of the Privacy Act of 1974.

Personnel Sensitive Examples: 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.

Business Sensitive Information or data is proprietary and must be protected from unauthorized access, to safeguard the privacy or security of Jefferson Science Associates (JSA) – including anything that poses a risk if discovered by a competitor or the general public. This information /data often has a time limit.

Business Sensitive Examples:
Commercial/proprietary – Trade secrets, business plans, facility floor plans and designs, cost data received from outside the company, personal statement, documents (inspection, reviews, site visits, investigations, audits, etc.) supplied by contractors and received in confidence.

Information Produced by TJNAF – Basic research, Cooperative Research and Development Agreements (CRADAs), Work for Other Agreements, TJNAF acquisition/evaluation plans, and results of evaluations and audits.

Intellectual Property – Contract negation information, procurement data, patentable design bids, R&D information, and pre-decisional information internal to TJNAF business communications or plans.

Personally Identifiable Information (PII) is any piece of information which can potentially be used to uniquely identify, contact, or locate a single person. Below is a list of items currently classified by JLab as PII. This list is not intended to be a comprehensive list, and it is anticipated that the list may change as the cybersecurity situation evolves.

Some Examples of PII include:

1. Complete Social Security Numbers in any form are PII (Taxpayer ID, Student ID, Driver's License Number)
   Date and place of birth (both together, not one by itself) associated with an individual
2. Mother's maiden name associated with an individual
3. Medical history information associated with an individual
4. Significant accumulations of personnel information can be considered PII, even if the contents are not explicitly listed in this document.
5. Financial information associated with an individual

    1. Credit card numbers
    2. Bank account numbers

For more information about PII at the Lab's, please visit the Service Now Center for full Policy and Definitions.

Pay Transparency Nondiscrimination Provision
JSA will not discharge or in any other manner discriminate against employees or applicants because they have inquired about, discussed, or disclosed their own pay, or the pay of another employee or applicant.

However, employees who have access to the compensation information of other employees or applicants as a part of their essential job functions cannot disclose the pay of other employees or applicants to individuals who do not otherwise have access to compensation information, unless the disclosure is (a) in response to a formal complaint or charge, (b) in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or (c) consistent with the contractor's legal duty to furnish information.

I understand that failure to comply with this agreement will result in

disciplinary action, up to and including termination.

Click here to sign

December
2023