



Safeguarding Confidential Information

Policy Number: 05-001

Research/Academic Policy

Effective Date: 1/4/2005

Responsible University Officer

- Chancellor
- Facility Security Officer

Responsible Offices

- Office of Research Integrity
- Office of Intellectual Property & Licensing
- Information Transfer and Security Committee

Related Policies

- Export Management

Policy Statement:

In conducting research and teaching activities involving the use of confidential information, University of Alaska Fairbanks institutes, departments, units, and employees must comply with all applicable University policies and procedures and contractual agreements, state and federal laws and regulations. As part of the University's Quality Improvement Program, all faculty, staff, students, and affiliates (including non-UAF consultants, collaborators, etc.) engaging in activities (research, consulting, advising, provision of service, etc.) involving confidential information, shall work under an Information Security Plan (ISP) which has been approved, in writing, by the Information Transfer and Security Committee (ITSC) prior to the commencement of the activity. The University of Alaska Fairbanks Chancellor, or a senior administrator formally designated by the Chancellor, will serve as the Institutional Official charged with the establishment and maintenance of appropriate administrative processes and procedures, described herein, to implement this policy.

Background:

The University has contractual obligations to program sponsors (government funding agencies, corporations, companies and individuals) to protect confidential information from unauthorized disclosure or access. Risk of unauthorized disclosure of or access to confidential information is associated with transmission, storage, distribution, and use of confidential information. Appropriate policies, procedures and physical security devices must be put in place and all applicable staff trained prior to receipt of any confidential information.

Whenever possible, the applicable security program should be included by reference in any contractual agreement. This will insure that all parties to the contract fully understand the requirements and obligations associated with the contract from the outset.

Definitions:

- **Authorized Personnel/User** refers to any person authorized by the Information Transfer and Security Committee, Office of Intellectual Property & Licensing or the FSO to work with confidential information. This includes, but is not limited to, University faculty, staff, students and volunteers.
- **Confidential Information** is any information, documents or materials in any form and however disclosed that is not intended for general distribution and is marked by the provider as proprietary or confidential (including United States government confidential, secret and top secret designations).
- **Contractual Agreement(s)** refers to any legal document(s) that obligate the parties to certain agreed upon conditions. “Contractual Agreements” may include, but are not limited to licensing agreements, non-disclosure agreements, government funding agency agreements and private company/corporation contracts for materials or services.
- **Facility Security Officer (FSO)** is the individual identified on the University of Alaska Fairbanks’ Facility Clearance as the point of contact for Defense Security Service communications. The duties of the FSO are defined by the National Industrial Security Program (NISP) and National Industrial Security Program Operating Manual (NISPOM). This position deals with government classified information (confidential, secret and top secret).
- **Information Security Plan (ISP)** is the specific policies and procedures established by a UAF institute, unit, department or program to prevent unauthorized access or disclosure of confidential and/or export controlled information and approved by the Information Transfer and Security Committee. At minimum, the ISP must identify a documentation manager, include physical security requirements, provide guidance for identifying authorized personnel, specify training requirements for authorized personnel and provide specific procedures for record keeping, storage, use, distribution, transmission, destruction and export of confidential information. In addition, the ISP must identify the lines of authority for all authorized personnel. The ISP must be auditable and an audit/assessment schedule must be identified.
- **Information Transfer and Security Committee (ITSC)** is the committee appointed by the Institutional Official which is responsible for reviewing and tracking all ISPs.
- **Office of General Counsel (OGC)** refers to the University of Alaska’s Office of General Counsel.
- **Office of Intellectual Property & Licensing (OIPL)** - the Director of OIPL may serve as a University signatory for the purposes of negotiating and signing contractual agreements. This office works closely with the Office of General Counsel, Office of Research Integrity and the Information Transfer and Security Committee.
- **Office of Research Integrity (ORI)** is the office responsible for ensuring compliance of University of Alaska Fairbanks personnel with internal policies and with local, state and federal regulations governing the conduct of research.
- **UAF Quality Improvement Program** is administered by the Office of Research Integrity. As part of this program, routine surveys and internal assessments are conducted in all research laboratories and facilities where confidential information is used and stored. The primary purpose is to ensure knowledgeable use of confidential information, adequate

security, proper record keeping and adherence to all university policies and procedures, government laws and regulations, and contractual agreements.

Responsibilities:

Obligations of the Administration and University Members

It is the responsibility of the Institutional Official, Information Transfer and Security Committee, the Office of Research Integrity and the Office of Intellectual Property & Licensing, as well as all units managing or conducting activities involving confidential information to support and protect both UAF and other party confidential information from unauthorized access or disclosure.

All university faculty, staff, students, and affiliates (including non-UAF consultants, collaborators, etc.) participating in research programs involving confidential information, other than U.S. government classified, shall work under an approved Information Security Plan (ISP) and shall receive any training, including continuing education, deemed necessary by the Institutional Official, ITSC or ORI regarding the safeguarding of confidential information.

Principal Investigator

For programs involving confidential information Principal Investigators shall:

1. submit an Information Security Plan (ISP) to the ORI;
2. receive written approval of the ISP prior to accepting confidential information;
3. keep ORI and the ITSC apprised of any changes in personnel and/or their citizenship status;
4. have all personnel approved by the ITSC prior to allowing them access to confidential information;
5. submit and receive written authorization from the ITSC for any changes/modifications to a previously approved ISP prior to their implementation; and
6. in cases where the confidential information is also export controlled, abide by UAF Policy: Export Management.

Institutional Official

For programs involving confidential information the Institutional Official shall:

1. work with the OGC, ORI and OIPL to ensure compliance with all applicable laws and policies;
2. formally appoint the members of the ITSC and designate the chairperson;
3. have approval authority for all administrative procedures necessary to implement this policy;
4. implement this policy with the assistance of the ITSC, ORI, and OIPL.
5. conduct an annual review of procedures, forms, etc. applicable to the implementation and administration of this policy;
6. take any actions, including revoking approval of an ISP or activity previously approved by the ITSC, that are in his/her judgment necessary to ensure compliance with applicable federal or state laws and regulations or university policies and procedures; and

7. work with the OGC to report any issues of noncompliance to the appropriate government regulatory and enforcement agencies.

The Institutional Official does not have authority to approve an ISP or activity that has been denied by the ITSC.

Information Transfer and Security Committee

For programs involving confidential information the Information Transfer and Security Committee shall;

1. review all ISPs submitted from UAF personnel;
2. have final authority to approve, require modification(s) in, or deny an ISP;
3. track the status of all ISPs and conduct continuing review of previously approved ongoing activities at least annually;
4. implement this policy with the administrative support from the ORI;
5. report as necessary to the Institutional Official;
6. initiate an inquiry in response to substantiated allegations of noncompliance and, when warranted, make recommendations regarding corrective or remedial actions to the Institutional Official;
7. take any action(s), including revoking approval of an ISP, suspending an activity or stopping funding, that are in its judgment necessary to ensure compliance with applicable federal, state, or university policies, procedures, laws and regulations; and
8. advise the Institutional Official on all aspects of the implementation of this policy and the applicable parts of the UAF Quality Improvement Program.

The ITSC has additional responsibilities with respect to ISP review specified in UAF Policy: Export Management.

Office of Research Integrity

For programs involving confidential information the Office of Research Integrity shall:

1. develop administrative procedures and forms for the implementation of this policy;
2. serve as administrative support for the Institutional Official and ITSC;
3. serve as point of contact for principal investigators, program heads and documentation managers;
4. maintain current copies of all approved ISPs and associated records;
5. assist principal investigators or program heads regarding all procedures and forms involved in the implementation of this policy; and
6. whenever necessary, obtain records and other relevant information related to the use and distribution/dissemination of confidential information;
7. coordinate information security training activities on behalf of the Institutional Official and ITSC;
8. conduct preliminary fact-finding regarding allegations of noncompliance and prepare a preliminary report for the ITSC;
9. to ensure compliance with applicable federal, state, or university policies, procedures, laws and regulations in cases of known or suspected noncompliance, the ORI has authority to temporarily suspend an activity, pending full review of the incident by the ITSC; and
10. implement the UAF Quality Improvement Program on behalf of the ITSC.

Non-Compliance:

Failure to comply with this policy, associated procedures, or to fully participate in the UAF Regulatory Compliance Self-Assessment Program is grounds for disciplinary action by the university and, if applicable, suspension or termination of research involving confidential information. Further action may include, but is not limited to, notification of any applicable funding sources and/or individuals, companies or corporations involved in the project through a contractual relationship, referral for misconduct proceedings, and/or reporting to state and federal authorities. Any disciplinary action taken by the University will follow the employment rules governing the individual's employment category.

Procedures:

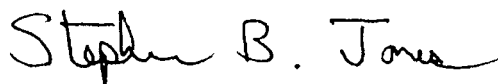
Administrative procedures and forms for the implementation of this policy will be formulated, maintained and distributed by the ORI. The ORI shall administer this policy on behalf of the Institutional Official and handle all correspondence between university personnel (faculty, staff, students, and affiliates) and the ITSC and Institutional Official.

Exclusions:

This policy does not apply to personal confidential information collected as part of research involving human subjects, student records or personnel files; all of which are covered separately. Specific policy concerning the protection of personal information collected as part of an approved research program involving human subjects is subject to approval and oversight by the Institutional Review Board. See UAF Policy: Research Involving Human Subjects.

All classified activities are covered separately and are subject to review by the facilities security officer.

Approved by:



1/4/05

Stephen Jones, UAF Chancellor

Date