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

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 polices and procedures; and

Non-Compliance:

Failure to comply with this policy, associated procedures, or to fully participate in the UAF Regula