GUIDELINES FOR HANDLING THIRD PARTY INFORMATION THAT IS TO BE PROTECTED PURSUANT TO AGREEMENT

In the course of conducting Illinois Institute of Technology ("IIT") business, IIT faculty and staff members as well as certain students, such as research assistants and student workers, are responsible for complying with the terms of contracts or agreements that limit access to or the ability to disclose confidential and/or proprietary information provided by, belonging to or collected on behalf of another organization (hereinafter, collectively "Confidential Information"). All individuals having access to such information are expected to educate themselves about the contractual limitations and obligations imposed on the Confidential Information to which they have access. Examples of the types of contractual arrangements that likely contain such provisions are:

- Non-disclosure (Confidentiality) Agreements pursuant to which confidential and proprietary information developed by or belonging to another entity is shared with individuals at IIT;
- End user licensing agreements associated with commercial software, shareware, freeware and other software used by IIT faculty members, staff members and students; and
- Contracts with external entities requiring compliance by IIT faculty members, staff members or students with security standards for an industry or association.

In order to assist IIT faculty and staff members as well as affected students with fulfilling their obligations to maintain the confidence of such information pursuant to these agreements, the following guidelines are being provided. These guidelines are <u>not</u> a substitute for the specific obligations contained in any such agreement, which are to be strictly followed. Rather, they are intended to provide a general framework to be considered by IIT faculty and staff members as well as affected students as they develop specific processes and procedures to fulfill their contractual obligations for handling/protecting such Confidential Information.

1. The lead individual or individuals responsible for ensuring compliance with the contract or agreement (e.g., Principal Investigator, lead negotiator, department supervisor, or such other individual) (hereinafter, each a "Responsible Party") should personally understand the restrictions on the access to and use of the Confidential Information as defined by relevant contractual obligations.

2. The Responsible Party should ensure that the applicable restrictions on the access and use of such Confidential Information are effectively communicated to all those who will use, administer, capture, store, process or transfer the information in any form, physical or electronic.

3. The Responsible Party should ensure that each user of the Confidential Information understands his or her information security-related responsibilities. All such responsibilities should be clearly communicated prior to sharing any Confidential Information. Ideally, these responsibilities should be explained orally and followed up in a written summary, which may be in the form of an e-mail.

4. The Responsible Party should ensure that individuals are permitted to access and use only such Confidential Information as is necessary for each of them to perform their legitimate duties and only when authorized by the Responsible Party.

5. Each user of Confidential Information should always ascertain and understand the sensitivity level of information to which he or she has access. No one should ever seek access to or use Confidential Information without authorization from the appropriate Responsible Party.

6. Individuals should no way divulge, copy, including placing it on a thumb drive, release, sell, loan, reverse-engineer, alter or destroy any Confidential Information, except as expressly authorized by the Responsible Party. As a general rule, Confidential Information should not be removed from the IIT campus. This means that Confidential Information generally should not be brought on travel, domestic or foreign, except at the expressed direction of the Responsible Party.

7. Individuals must adhere to IIT requirements (as set forth in IIT's *Policy on the Use of Technology Resources*) for protecting any computer used to conduct IIT business.

8. Individuals should protect the confidentiality, integrity and availability of Confidential Information as appropriate for its sensitivity level and the format in which the Confidential Information is maintained, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, or by any other means.

9. Individuals should safeguard any physical key, ID card or computer/network account that allows them to access Confidential Information. This includes creating difficult-to-guess computer passwords.

10. At the end of the relationship allowing access to and use of Confidential Information, IIT personnel will be expected to return, destroy, or render unusable or inaccessible, any Confidential Information contained in any physical document (e.g., memos, reports, microfilm, microfiche) or any electronic, magnetic or optical storage medium (e.g., USB key, CD, hard disk, magnetic tape, diskette). The agreement creating the obligation of confidentiality may well indicate whether information is to be returned or destroyed and the means for doing so.

11. Individuals should immediately report to the Responsible Party any activities that they suspect may compromise the security and/or protection of Confidential Information.

12. Confidential Information should always be stored in a safe, secure (locked) location, such as a locked filing cabinet, locked desk door or on a computer that is protected with a strong password and configured to "time out" after no more than 20 minutes of inactivity. If the Confidential Information is being stored in a physical location, it should be returned to that location when the user is finished. Confidential Information should never be left out or left unattended. If the Confidential Information is stored on a computer, a user should lock or log off the computer before leaving it unattended, ensure that system and application security updates are applied as soon after being released by the vendor as possible, and ensure that anti-virus software is installed and is actively protecting the system.

13. Conversations regarding Confidential Information should not take place in public places or in other locations where they can be reasonably overheard, such as in an office with the door open, or in the presence of individuals who do not have the right to access and use Confidential Information.

14. When Confidential Information is stored on a computer, laptop or other mobile device or is being electronically transmitted, the user should consider using reasonably appropriate encryption methods/technologies.

15. All individuals should remember that their obligation to protect Confidential Information continues after they leave IIT.

16. While federal and state laws create certain exceptions allowing for the disclosure of Confidential Information in order to comply with investigative subpoenas, court orders and other compulsory requests from law enforcement agencies, anyone who receives such compulsory requests should contact the Office of General Counsel before taking any action.