I. User Responsibility

A. The proper use of all IIT computer accounts and technological resources, including computers, E-mail, Google Apps for Education, Internet, printers, software, servers, voice and data networks, including Voice over Internet Protocol (VoIP) – the polices for which are outlined in Exhibit II and are an express part of this policy, information systems and any and all other computer peripherals (collectively, "Technology Resources"), is the personal responsibility of each individual. Use of Technology Resources, whether by faculty, students or staff (collectively, "Users"), must be consistent with institutional policies governing the conduct, including those regarding plagiarism, discrimination, cheating, harassment and theft. Users must never represent or imply that the opinions that they express on or through Technology Resources are the views of IIT.

B. Technology Resources are made available to support the academic mission, programs and activities of IIT. Use of Technology Resources is a privilege that is not to be abused, and it can be taken away without prior notice and consent or when required by law or when a substantiated reason exists to believe that violations of law or policy have occurred. In time-sensitive cases, access may be restricted to meet critical operational needs. Any inappropriate, illegal, unethical or immoral use constitutes a violation of this policy regardless whether it is specifically identified herein.

C. Each User is responsible for the storage of personal files created on IIT Technology Resources. Hard drives and other means of storage are routinely cleared of files. IIT will not be liable, under any circumstances, for files stored on or deleted from its hard drives or other means of storage.

D. Passwords are one of the primary mechanisms that protect IIT's Technology Resources from unauthorized use. Thus, constructing secure passwords and ensuring proper password management are essential; poor password management and construction can allow both the dissemination of information to undesirable parties and unauthorized access to IIT Technology Resources. As poorly chosen passwords are easily compromised, standards for proper password creation and management reduce these risks. Accordingly, IIT has established minimum standards for password creation and management. These standards, which are attached to this policy as Exhibit I, apply to all Technology Resources that a User, whether students, faculty members and staff, may access and/or utilize, and it is required that each User comply with these minimum standards so as to ensure that IIT Technology Resources are protected by strong passwords. Further, each User is responsible for taking reasonable care for the security of his or her campus accounts and passwords. For example, one should change his or her passwords frequently and not employ an obvious or simple password (e.g., your name, your pet's name or your

birthdate). One should not under any circumstances give his or her passwords to another person. As set forth in Exhibit I, system and application developers shall avoid creating applications which store passwords. If password storage cannot be avoided, application developers must ensure that applications do not store passwords in clear text or an easily decrypted format. Finally, each User must also recognize that IIT has limited means of preventing unsolicited communications from within and outside of the IIT network. Users who receive threatening or inappropriate communications should bring them to the attention of the appropriate network administrator, Office of General Counsel, Office of Human Resources or the Office of Student Affairs.

II. Examples of Appropriate Uses of Technology Resources Include, But Are Not Limited To:

A. Faculty and student research;

B. Class assignments; and

C. Instructional uses.

III. Examples of Inappropriate Uses of Technology Resources Include, But Are Not Limited To:

A. Using Technology Resources for commercial purposes;

B. Sending unsolicited, annoying or obscene messages or E-mail to another computer or computer user;

C. Utilizing a false identity in obtaining or utilizing an E-mail account or to gain access to a Technology Resource;

D. Displaying adult web sites (especially those self-identified as such) or other obscene materials in public computer laboratories;

E. Examining or attempting to examine another user's files, accounts or E-mail, without explicit permission by the owner of those files or E-mail;

F. Interrupting, hindering, damaging or otherwise interfering with the normal operation of the computer laboratories, systems, wired and/or wireless data networks and voice systems, including, but not limited to, port scanning, IP spoofing, network analysis, network monitoring, illegal logins, running traffic-generating applications, installing any software or program code that is intended to or likely to result in the eventual damage to or degradation of the performance of Technology Resources, or using Technology Resources to perform acts that are deliberately wasteful of computing resources;

G. Posting copyrighted text or images on a webpage without the owner's permission or in any other way violating copyright laws, including, but not limited to, the use of peer-to-peer file sharing applications to illegally transmit music, software, movies or other protected materials; and

H. Using Technology Resources to engage in or further any fraudulent or criminal act or to violate IIT policies, including, but not limited to, monitoring, in any way, another User's data communications, gaining or attempting to gain access to remote computers, infringing the rights of other Users to use Technology Recourses, or violating the terms of software licensing agreements.

For the avoidance of doubt, nothing in this section is intended to limit or restrict the ability of an employee from engaging in protected, concerted activities.

IV. Privacy Issues and Access to Files

A. Users have only a limited right to privacy in their electronic and voice mail. IIT does not monitor, review or perpetually archive material prior to or after transmission on Technology Resources. Authorized IIT staff will treat all electronically stored information as confidential, but they may have access to, examine and/or disclose information when (i) the owner of the information authorizes disclosure, (ii) a User is suspected of violating IIT policies or local, state or federal law, including, but not limited to, laws regarding harassment, copyright, libel and defamation of character, (iii) administrators are performing routine or necessary services to maintain or enhance the operations of the Technology Resources, (iv) exigent circumstances exist such that access is deemed reasonably necessary to prevent injury, loss of life, property damage, or significant disruption to university operations, or (v) an employee is terminated and his or her files are need in the course of operations at IIT.

IIT's E-mail and Google Apps services are remotely hosted by Google, and hosting can occur at one or more Google facilities located throughout the world. Google reserves the right to administer all accounts in accordance with the Google Terms of Service (http://www.google.com/intl/en/policies/terms/).

B. The Google Apps for Education system at IIT exists to provide a convenient (not confidential) way of communicating between students and faculty, between colleagues and friends. It is expected that Users will use common courtesy in the use of E-mail. Examples of inappropriate use include, but are not limited to:

(1) Re-posting (forwarding) personal communication, intended to be confidential, without the author's prior consent;

(2) "Chain letters," "broadcasting" messages to lists or individuals, and other types of use which would cause congestion of the networks or otherwise interfere with the work of others are not allowed; and

(3) Anonymous and/or fraudulent posting of email messages.

C. Google Apps provides tools for public communication and cannot be guaranteed to be private. Users are advised to be discreet. Issues of personal privacy and data confidentiality are important to IIT. Generally, personal data will only be accessed in accordance with Section IV.A. Systems and network administrators do have access to files in the IIT Google Apps environment. In the course of routine system maintenance, trouble-shooting and mail delivery problem resolution, staff

may see the content of email messages; however, these individuals are prohibited from accessing personal files except as otherwise stated Section IV.A.

D. Google Apps accounts for students and employees are provisioned, maintained and disabled in accordance with the IIT Employee Google Apps Account and Usage Procedures and IIT Student Google Apps Account and Usage Procedures available at http://www.iit.edu/ots/our_policies.shtml

V. Intellectual Property

As indicated in Sections III.G and III.H, it is a violation of this Policy to use IIT Technology Resources to engage in any activity that would infringe or violate the copyrights or other intellectual property interests of others. All communications and information accessible via the Internet should be assumed to be copyrighted and should be accessed and re-distributed only in accordance with copyright rules. When sources found on the Internet are cited, the name, date and location of the information must be included.

IIT reminds students, faculty and staff that it is a violation of federal law to infringe or violate another party's copyright. Owners of registered copyrights can enforce their rights by bringing a civil suit. In addition, criminal prosecution can be brought by the United States Attorney, and Customs and Postal officials may seize and impound infringing articles. The penalties for infringement can be substantial. In civil actions brought by the copyright owner, a court may order forfeiture and/or destruction not only of all infringing articles but also of any implements used to manufacture the infringing articles. In addition to obtaining an order stopping the infringement and ordering destruction of infringing articles, the court can order payment of any provable damages, including lost profits. The copyright owner can elect to receive "statutory damages". The minimum amount of statutory damages that can be awarded for copyright infringement is $750; the maximum amount is $30,000. If the infringement was willful, the potential statutory damage award is increased to $150,000 for each act of infringement. In addition, attorneys' fees may be awarded. Further, all willful copyright infringement is a criminal offense, subject to prosecution. The criminal penalties for a first time conviction for willful infringement range, on the low end, from a prison sentence of up to one year and a fine of up to $5000 to five years in prison and a fine of up to $250,000 on the high end. Second and subsequent offenses can carry a prison term of up to ten years in addition to the fine.

VI. Web Page Responsibilities

The Office of Technology Services (OTS) and the Center for Law and Computers (CLC) have devised specific rules and procedures applicable to IIT-related web pages. All web pages contained within the iit.edu and kentlaw.edu domains or served on IP addresses owned by IIT are subject to the following content guidelines, as well as all other applicable IIT policies.

A. OTS and CLC are responsible for the web servers only, including maintenance, infrastructure and reasonable security. OTS and CLC are not responsible for any web page content or hyperlinks. Links from www.iit.edu and

www.kentlaw.edu main pages to the organization and department pages are maintained by the Office of Communications and Marketing at the Main Campus and the Office of Public Affairs at the Downtown Campus.

B. The content of the first-level pages on the IIT web site, http//www.iit.edu, is designed and specified by the Office of Communications and Marketing, and the content of the first-level pages on the Chicago-Kent web site, http//www.kentlaw.edu, is designed and specified by the Office of Public Affairs.

C. All other web pages contained within, except for individual faculty, staff and student pages, should follow the design standards set forth by the Office of Communications and Marketing and the Office of Public Affairs, as applicable.

D. All pages must clearly display at the bottom of the page the name and email address of the person responsible for the page.

E. Pages cannot contain or transmit any information that is illegal, pornographic, defamatory, obscene or harassing.

F. Users are prohibited from serving pages that conduct electronic commerce or contain paid advertising. Pages must not cause interference with the ability of other users to access network resources.

G. Pages that do not meet acceptable use or content standards are subject to immediate removal, and Users are subject to the suspension of web privileges as well as further disciplinary procedures as appropriate.

H. Student organizations and private, individual pages should link to a disclaimer stating that the content does not express the views of IIT.

VI. Enforcement and Compliance Procedure

A. Each university department/unit is responsible for implementing, reviewing and monitoring internal policies and practices to assure compliance with this policy. The Chief Information Officer is responsible for enforcing this policy and is authorized to set specific password creation and management standards for university systems and accounts.

B. Inappropriate uses of Technology Resources should be reported to the Office of Technology Services via abuse@iit.edu. Security related questions and issues should be directed to security@iit.edu. Anyone discovered to be hindering normal operations, making inappropriate use of Technology Resources or acting in a manner contrary to this policy will be contacted and appropriate action taken, including, as appropriate, disciplinary action consistent with applicable policies and procedures. Further, in order to protect IIT's Technological Resources and the ability of others to use the same, upon report or discovery of such a violation, the User may be immediately and without warning denied access to IIT Technology Resources, as and to the extent deemed necessary or appropriate to maintain the security thereof, which denial of access may remain until the violation has been rectified. All pertinent information on the alleged violation will be given to the

appropriate IIT official who may then take action in accordance with applicable policies.

C. Exceptions to the password security protocols established by Section I.D of this policy may be granted by the Chief Information Officer or designee, in his/her discretion, in cases where security risks (i) are mitigated by alternative methods, or (ii) are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate academic or business needs. Such an exception must be requested in advance. To request a security exception, contact the Support Desk by calling (3212-567-DESK), emailing (supportdesk@iit.edu) or stopping by the 2nd Floor Galvin Library.

EXHIBIT I
MINIMUM STANDARDS FOR PASSWORDS

1. Password Construction

1.1 Minimum Password Length. Passwords shall have a minimum of eight characters and a maximum of 30 characters with at least one upper case letter, one lower case letter, one number, and one special character that may not include @, #, any other unicode or $ as the first character.

1.2 Password Composition. Passwords shall not consist of well-known or publicly posted identification information. Names, usernames, and A-numbers are all examples of well-known identification information that should not be used as a password. Additional helpful hints on password construction can be found in Appendix A - Password Construction Tips, which follows this Exhibit I.

2. Password Management

2.1 Password Storage. Passwords shall be memorized and never written down or recorded along with corresponding account information or usernames. Passwords must not be remembered by unencrypted computer applications such as email. Use of an encrypted password storage application is acceptable, although extreme care must be taken to protect access to said application.

2.2 Password Aging. General IIT community members must change their passwords at least once every 365 days with the exception of administrators and IT staff that handle sensitive data, who must change their passwords every 90 days.

2.3 Password Reuse. Care shall be taken to prevent the compromise of one username/password from compromising the security of multiple systems or resources. Users shall not use the username and password combination from any non-IIT account as the username and password for their IIT accounts. Further, you may not reuse passwords for the same account.

2.4 Password Sharing and Transfer. Passwords shall not be transferred or shared with others unless the User obtains appropriate authorization to do so. When it is necessary to disseminate passwords in writing, reasonable measures shall be taken to protect the password from unauthorized access. For example, after memorizing the password, one must destroy the written record. When communicating a password to an authorized individual orally, measures must be taken to ensure that the password is not overheard by unauthorized individuals.

2.5 Electronic Transmission. Passwords shall not be transmitted electronically over the Internet using insecure methods. Wherever possible, security protocols including IMAPS, FTPS, HTTPS, etc. shall be used.

3. Requirements for System Administrators

3.1 Require Passwords for Login. Systems shall not be configured to allow user login without a password. Exceptions shall be granted for specialized devices such

as public access kiosks when these devices are configured with public user accounts that have extremely restricted permissions (e.g., web only) that are separate from administrative accounts.

3.2 Protect against Password Hacking. System administrators shall harden their systems to deter password cracking by using reasonable methods to mitigate "brute force" password attacks. For example, IIT may choose to configure the system in such a way that after five failed attempts to log-in one would be unable to proceed with login. IIT may also introduce a time limit before allowing another login attempt.

3.3 Logging. Practicable measures shall be put in place to log successful and failed login attempts.

3.4 Changing Password after Compromise or Disclosure. System administrators shall, in a timely manner, reset passwords for User accounts or require Users to reset their own passwords in situations where continued use of a password creates risk of unauthorized access to the computing account or resource. Examples of these situations include, but are not limited to: disclosure of a password to an unauthorized person; discovery of a password by unauthorized person; system compromise (unauthorized access to a system or account); insecure transmission of a password; replacing the User of an account with another individual requiring access to the same account; password is provided to IT support staff in order to resolve a technical issue; and account password is communicated to a User by the system administrator.

3.5 Default Passwords. System administrators and IT personnel shall not use default passwords for administrative accounts.

4. Requirements for Application Developers

4.1 Require Secure Transmission. Application developers shall, whenever possible, develop applications that require secure protocols for authentication.

4.2 Storing Passwords. Application developers shall avoid creating applications which store passwords. If password storage cannot be avoided, application developers shall ensure that applications do not store passwords in clear text or an easily decrypted format.

4.3 Unique User Accounts and Passwords. Applications shall support unique user accounts and passwords so that individual Users are not required to share a password in order to use the application.

4.4 Use myIIT Portal Whenever Possible. Applications shall, whenever possible, use the User's myIIT portal password for authenticating members of the IIT community instead of creating another unique ID or username.

Appendix A
Password Construction Tips

- Acceptable Methods to Create a Strong Password
  - Use a minimum of 8 characters. Generally, the more characters you use, the harder a password is to be cracked or guessed.
  - Choose a password that is easy for you to remember but would be hard for another to guess. One useful approach is to use a sentence or saying to create a "passphrase" by using the first letters, capitalization and special characters as substitutes. For example, "One ring to rule them all, one ring to bind them" may be used to create a passphrase like "1R2rtAor2Bt" that can be used as a very strong password.
  - Use mixed case (upper & lower) and numbers.
  - Use special characters and/or punctuation symbols (Examples include: _ - + = ! % * & " : . /). Do not use @, #, any other unicode, or $ as the first character.

- Unacceptable Methods to Create a Strong Password
  - Do not use words, numbers or known or public information associated with you (e.g., Social Security numbers, names, family names, pet names, birthdays, phone numbers, addresses, etc.).
  - Avoid using your login name or any variation of your login name as your password. If your login is 'fredrick', do not use substitution or letter reordering. Examples would be 'fr3dr1ck', where the 3=e and the 1=i. Further, do not use kcirderf (backwards) or add a digit to the beginning or end of the word (1fredrick or fredrick1).
  - Do not use the same character for the entire password (e.g., '11111111') or use fewer than eight unique characters.
  - Do not use common letter or number patterns for your password (e.g., '12345678' or 'abcdefgh').
  - Substitution should not be used on common words or with common substitutions (e.g., 3=E, 4=A, 1=I, 0=O, etc.).
  - When changing a password, change to an entirely new password. Do not just rotate through a list of favorite passwords.

EXHIBIT II
POLICIES AND PROCEDURES FOR USE OF VOICE OVER INTERNET PROTOCOL

IIT provides faculty, staff and students access to Voice over Internet Protocol ("VoIP"). VoIP is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, most commonly the Internet. IIT provides VoIP through a subscription it has with a third-party provider (said provider along with its licensors, hereinafter collectively referred to as the "Provider"). In connection with this subscription, IIT is obligated to ensure that certain policies, procedures and rules are adhered to when Users utilize the VoIP service. These policies, procedures and rules are set forth below, and all Users utilizing VoIP services must adhere to the same.

1. The Services

1.1 Each user agrees that the Provider retain all proprietary right, title, and interest, including copyright and all other intellectual property rights, in and to the VoIP services as they currently exist or as modified, including, without limitation, in and to any readable features such as documentation, reports, menus, audible prompts, and tone sequences that the User's can access and use in connection with the VoIP services. For the avoidance of doubt, User's use of the Services shall in no manner entitle the User to a claim of ownership in the Services.

2. Code of Conduct and Acceptable Use

2.1 Each User agrees to abide by the following rules in connection with User's access to and/or use of the VoIP services:

(1) User is responsible for making sure User is dialing from the correct line on User's assigned SIP phone. User must not alter the connection for User's assigned SIP phone without permission from IIT's Office of Technology Services.

(2) User must not attempt to undermine the security or integrity of the VoIP services or any related networks nor cause the disabling or circumvention of any security mechanism contained in or associated with the VoIP services. User must not attempt to gain unauthorized access, nor attempt, whether through use of disassemblers or any other means whatsoever (including, but not limited to, manual, mechanical, or electronic means) to adapt, alter, modify, copy, reproduce, distribute, transcribe, translate, reduce, reverse engineer, decompile, disassemble, display or attempt to generate or access the source code, algorithms, structure or organization of any of the VoIP services, the Provider's software, or any other software used by the Provider to provide the platform for the VoIP services, in whole or in part, unless expressly permitted by applicable law. User must not prepare derivative works from any component of the VoIP services. User must not delete, alter, cover, or distort any copyright or other proprietary notices or trademarks.

(3) User may only use the VoIP services for lawful purposes and in accordance with all applicable laws and regulations. For example, use of the VoIP services to transmit any material in violation of any applicable law or regulation is prohibited. Such prohibitions include, without limitation, material protected by copyright, patent, trademark, trade secret, or other intellectual property rights used without proper authorization, and material that is obscene, libelous, or defamatory, constitutes a threat or harassment, or violates export control laws.

(4) User acknowledges that the VoIP services are not designed, manufactured, or intended for use or resale as online control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation, or communication systems, air traffic control, weapons systems, or direct life support machines, in which the failure of the software could lead directly to death, personal injury, or severe physical or environmental damage.

(5) User must not restrict or inhibit any other User from using the VoIP services; however, User may not sell, lend, rent, give, assign, or otherwise transfer or provide access to the VoIP services to a third party or commercially exploit the VoIP services by marketing, licensing, selling, distributing, or transferring the VoIP services to a third party.

3. Suspension and Termination of User's Use of the Services

3.1 If any User breaches or violates the terms and conditions set forth in this Exhibit II or elsewhere in this Policy, it is expressly understood by User that his or her access to and use of the VoIP services may be suspended or terminated without prior notice to User. In addition, User's access to and use of the VoIP services may be suspended or terminated without prior notice to the User in the event IIT or Provider deems it necessary and acceptable to do so. The terms of this Section 3.1 are set forth in IIT's Contract with the Provider, and as such, they are not waivable by IIT. User's are hereby expressly informed that enforcement of the Provider's rights hereunder is within the sole discretion of the Provider.

4. Sanctions, Disciplinary Actions, and Legal Actions

4.1 Without limitation of the Provider's other rights or remedies as set forth herein or IIT's rights under this policy or any other applicable policy, User acknowledges and agrees that a breach by User of these VoIP policies and procedures may result in (i) IIT imposing sanctions on the User's use of the VoIP services, (ii) IIT initiating disciplinary action against the User in accordance with university policies, and/or (iii) legal action by the Vendor against the User.

4.2 Any information and/or complaints regarding violations of the terms set forth in this Exhibit II should be directed to: abuse@iit.edu.