Technical Infrastructure Data Privacy, Safety, and Security Plan

Technical Infrastructure & Security

Except for LMS servers, IFTI uses technical infrastructure supplied by IUPAT under the terms of a long-term shared services agreement. The information systems services include, but are not limited to the support and maintenance of campus IT infrastructure. This includes evaluating new technology, server and PC hardware and software, networking, custom applications, digital and wireless telephones, document management, perimeter and digital security and audio and video needs.

The IUPAT IT infrastructure consists of an onsite and offsite data center for redundancy. The onsite data center is restricted by key and cardkey entry by authorized IUPAT employees. The site has multi-layer security systems including cardkey entry and indoor/outdoor video surveillance. The offsite data center is PCI, HIPAA, DIACAP and SSA16 Type I compliant. Access is restricted to authorized client personnel and authorized Xecunet employees only. The site has multi-layer security systems including cardkey entry, hand geometry readers, pin-code, man trap, and indoor/outdoor video surveillance. All records are protected by application security, which are backed up locally and replicated to the offsite data center for redundancy.

LMS servers are hosted at Amazon Web Services (AWS). AWS data centers are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Computer Usage

Computing equipment and services are provided solely for the use of authorized users, whether in headquarters offices or in any remote location. FTI-provided equipment and services are to be use only by persons specifically authorized by the employer. All equipment and any data processed or stored on the employer's equipment or system is the property of FTI. All software and other copyrighted materials are to be used in ways consistent with licensing or copyright restrictions. Employees must scan imported and downloaded files for

viruses before opening the files and exposing the system to the contents of the file. The IS Administrator will provide an individualized log-on script and personal password for each authorized user. All passwords are subject to periodic change by the employer. Employees are prohibited from disclosing their log-in name or password. All users must log-off the network and turn their machines off at the end of the workday. Employees shall promptly notify the IS Administrator of materials or activities that violate any portion of the employer's computer-use policies.

Expectation of Privacy

Employees should not have an expectation of privacy, even when computer files are password-protected. FTI reserves the right to inspect an employee's computer system and telephone for violations of policy.

Rules Governing Encryption

Encryption of files or email messages is expressly forbidden, unless authorized by the IUPAT, utilizing employer-provided encryption tools consistent with IUPAT security protocols. Employees who encrypt files must provide their immediate supervisor with a sealed hard copy record of all of the passwords and/or encryption keys necessary to access the encrypted files.

Internet Use

Access to Internet email, news groups, web sites, ftp file download sites, and computer "bulletin boards" or listserves will be provided for employees whose work requires such access, when authorized by a supervisor. All postings to public forums should include the following disclaimer: The contents of this message have not been reviewed by the employer. Alternate Internet service provider connections to the internal network are not permitted unless expressly authorized and properly protected by a firewall or other appropriate security device(s). Employees should be aware that many internet sites have software to identify the user, and the employer. It is expected that employees will behave responsibly. The employer has installed software that will monitor and record internet use. Authorized supervisors may periodically monitor content of messages and review the sites visited by employees. All internet data that is composed, transmitted, or received via the employer's computer communications system is considered to be part of the official records of the employer. Employees should always ensure that the business information contained in email messages and other transmissions is accurate, appropriate, ethical and lawful. The truth or accuracy of information on the internet and in email should be considered suspect until confirmed by a separate (reliable) source. As a general rule, if an email message does not require a specific action or response, it should be deleted after it is read. The employer may preserve all email messages for varying periods. Periodically all stored email messages will be deleted. The employer reserves the right to review, audit, intercept, access and disclose all messages received, created or sent over the e-mail system for

any purpose. Reports or audits of Internet usage may be prepared at the request of the Fund Administrator. Employees should not place material owned by the employer (copyrighted software, internal correspondence, etc.) on any publicly accessible internet computer without prior permission.

Personal Use

Electronic media and services are provided by the employer for employees' business use. All employees are responsible for their own productivity. Limited, occasional, or incidental use of electronic media for personal, nonbusiness purposes is understandable and acceptable, within the limits of applicable law, and the rules imposed by this and other policies of the employer. This means usage prior to or after your regularly scheduled work hours or during your lunch hour. Your supervisor must first approve any other personal use. The employer, at its sole discretion, reserves the right to review any employee's electronic files and messages, and to restrict the employee's access to electronic media and services.

Prohibited Uses

 Any use that interferes with productivity in the workplace, including excessive personal use.

 Any use of electronic media or services for any illegal purpose.

 Any activity that consumes system resources, including receipt or transmission of large personal files (photographs and sound files, for example).

 Any use for personal gain or profit.

 Any solicitation, including religious or political solicitation.

 Any fraudulent or harassing use, or use that is embarrassing to the employer.

 Any download, transmission, copying, or display of sexually explicit or offensive materials.

 Broadcast of "chain letters" or other unauthorized mass electronic mailing.

 Download or duplication of any music or other electronic files in violation of copyright rules.

 Download of any software without permission of the IS Administrator.

 "Hacking," including the unauthorized access to any computer, server, file or

 device.

 “Spoofing,” including attempts to hide the identity of the sender or efforts to represent the sender as someone else.

 “Snooping” or attempts to access others’ email or any electronic files except by authorized staff for business purposes.

 Any attempt to test, circumvent or defeat security or auditing systems without the permission of the IS Administrator.

Reserved Rights

The employer reserves the right to alter this policy at any time, and to limit or discontinue internet access as it sees fit. The employer reserves the right to take any permitted steps to maintain a productive workplace.

The Family Education Rights and Privacy Act of 1974

The Federal Family Educational Rights and Privacy Act (FERPA) of 1974 regulate a wide range of privacy related activities including:

 Management of student records maintained by the School

 Regulations regarding who has access to student records

 For which purposes access to student records is granted

School officials will release educational information upon receipt of a signed, dated, written consent of the student which must specify the records that may be disclosed and identify the party to whom the disclosure may be made, including:

 Parents of a dependent student, as defined by the Internal Revenue Code of 1954, Section 152 and who supply supporting documentation, may be granted access to a student's educational record under some circumstances.

 In connection with Financial Aid, to organizations who are conducting studies that are on behalf of educational agencies;

 _____To Federal or State educational authorities;

 To accrediting organizations;

 In compliance with a lawfully issued subpoena;

 In connection with a health or safety emergency.

Non-School individuals (including parents except as described above) *may not have access* to educational records other than Directory Information unless authorization from the student is obtained or a lawful subpoena/court order is issued to the School. Examples of records not released are grades; the specific number of hours/credits enrolled, passed, or failed; Social Security Number; student ID number; name of parents or next of kin; and/or residency status. **Students must complete a form authorizing the Administrator's Office to**

permit employers to view the student's academic record.