GUIDELINES ON USE OF INFORMATION TECHNOLOGY RESOURCES

Revised July 1, 2016

These Guidelines supplement University Policies and apply to all users of information technology resources, including all staff, consultants, contractors, student employees and temporary employees (collectively referred to as "Users") in all areas supported by Financial Information Systems (FIS). The goals of these Guidelines are the following:

- Provide guidance for permissible and impermissible uses of information technology resources
- Ensure the availability, integrity, and confidentiality of information assets
- Reduce risk of legal liabilities
- Comply with security standards, regulatory requirements, and laws
- Maximize the return on investments in information technology

Ownership

All computing and information devices, systems, software, peripherals, and data (collectively referred to as "IT Resources") are the property of the University of Pittsburgh. All data created on University IT Resources remains the property of the University of Pittsburgh. Information is an asset of the University, and all Users must protect this asset.

Appropriate Use

The University provides IT Resources for authorized business purposes only. IT Resources must not be used for personal financial gain, political purposes, or for the storage, transmission, or display of obscene materials. Minimal personal use of IT Resources such as phones, email and internet access is permissible if it does not interfere with work-related use of IT Resources.

Resource Management

FIS has the authority to manage all IT Resources within its service area. To ensure effective use of technology, IT Resources are allocated and replaced on a schedule determined by FIS.

Users are not permitted to buy, install, change, move, or dispose of any IT Resource, engage in IT-related contracts or hire IT consultants or employees without FIS approval. All agreements with third-party vendors and contractors must meet FIS IT guidelines and security standards. Any damage or loss of IT Resources must be reported to FIS immediately.

Software

Only software that has been properly licensed to the University, and approved and installed by FIS will be used. Users are not permitted to download software from the internet, or duplicate, store or distribute copyrighted materials or intellectual property. FIS may delete any non-approved software without notice.

Confidential Information

Confidential information is information disclosed or known as a consequence of employment or engagement with the University, and not generally known outside of the unit. Confidential information must be marked as such.

Users must keep confidential information secret and not disclose it in any manner, except as directed by an authorized individual. Users are not permitted to remove confidential material from the premises without approval by an authorized individual. Users must take reasonable actions to prevent disclosure, modification, destruction, and unauthorized access to confidential information; whether accidental or intentional.

Sensitive Data

FIS considers certain data sensitive and, as such, must be protected. Sensitive data includes the following:

- Account Passwords
- Biometric Identifiers
- Date of Birth / Death
- Employer Identification Numbers
- Financial Account Numbers
- Identifiable Human Subject Research Data
- Mother's Maiden Name
- Personal Identification Numbers
- Place of Birth
- State ID Card Numbers
- Bank Routing Codes / Account Numbers
- Credit / Debit Card Numbers
- Driver's License Numbers
- Encryption Keys
- Government-Issued ID Numbers
- Insurance ID Numbers
- Medical Record Numbers
- Protected Health Information
- Social Security Numbers
- Vehicle Identifiers

Users are permitted to collect, display, transmit and store sensitive data only if necessary for legal, regulatory, or legitimate business reasons and must use secure methods approved by FIS. Users must make every effort to limit display of sensitive data by masking or truncating the data wherever possible.

Users must ensure that all sensitive data, electronic or physical, is purged after it is no longer needed for legal, regulatory, or business reasons. All hard copies of sensitive data must be disposed of through cross-cut shredding or incineration so it cannot be reconstructed. Sensitive data stored on electronic media must be made unrecoverable through physical destruction when no longer needed.

Users must protect all payment card data in accordance with Payment Card Industry Data Security Standard (PCI DSS) requirements.

Access Control

Only authorized Users are permitted to access University IT Resources. All access to IT Resources must be approved by FIS and the data owner. Users must use only the devices, accounts, and information for which they are authorized. FIS manages all access to IT Resources and will provide access based on the least privileges necessary to perform job responsibilities.

Users are responsible for the security of their accounts and passwords; and for proper use of IT Resources assigned to them. All default or predefined passwords must be changed as soon as possible. All user accounts must be unique and not shared with others. Users must not share or provide access to IT Resources, private information, or identification such as usernames or passwords. Users must be aware of others who may be trying to view their passwords as they are entered.

Supervisors are responsible for ensuring that appropriate background checks are performed through Human Resources before hiring any employee that has access to sensitive data. Supervisors must immediately notify FIS when user accounts or access should be changed or terminated.

Access to IT Resources by third parties such as vendors, service providers, and business partners is controlled by FIS, and is only made available when needed and immediately deactivated after use. Inactive accounts and sessions will be terminated after a specific period of inactivity as determined by FIS.

Physical Security

Physical security of all IT Resources, whether University or personally owned, must be maintained.

Users must protect IT Resources from unauthorized physical intrusion, theft, and other hazards; and be aware of eavesdropping, "shoulder surfing", and the need to question strangers in offices or private areas. When leaving their work area, Users must secure workstations to prevent access to IT Resources by unauthorized individuals. This includes securing file cabinets, check stock, signature cartridges, University letterhead, form stock, check printers, currency, etc.

Users must secure all publicly-accessible IT Resources with physical locks, maintain key control, and use safeguards that limit access to sensitive areas only to individuals with appropriate clearance.

Security Management

All Users must complete the FIS online security awareness training course within the first thirty (30) days of hire, and a refresher training course annually thereafter. All IT Resources commonly affected by malicious software must use regularly-updated anti-virus software.

Users who learn of a possible security lapse or weakness relating to University IT Resources are required to immediately report the incident to their supervisor and to FIS. Evidence will be gathered, recorded, and retained by FIS. Evidence may also be shared with third parties and law enforcement as appropriate.

Users must not:

- Attempt to disclose, circumvent or disable security measures used on IT Resources
- Attempt to gain access to IT Resources that they are not authorized to access
- Accept any form of help to alter the security or configuration of IT Resources without the consent of FIS; this includes consulting services, remote assistance, or software installation

Email and Electronic Communication

Information obtained from internet or email sources should be verified before being used for business purposes. Users must treat unsolicited emails with caution and not respond to them. Users must be cautious of phishing attempts, malware, and links to malicious web sites. Users must delete suspicious file attachments without opening.

Users must not use email or other IT Resources to:

- Circulate chain letters, pyramid schemes, unsolicited mass mailings ("spam"), or alleged virus/security warnings
- Request non-University services, promote personal business, or sell/trade goods or services
- Send fraudulent, obscene, defamatory, or harassing communications
- Hide or misrepresent their identity

Mobile Devices

Mobile and wireless computing devices such as laptop computers, tablets, smart phones, or other hand-held devices must be password-protected and physically secure. Loss or theft of mobile devices must be reported immediately to FIS.

Users are required to backup information on their devices and install the latest operating system updates/security patches, on a regular basis.

Users may download mobile applications only from a reputable source and may connect mobile devices only to trusted wireless networks and computers.

Users are not permitted to store sensitive data on mobile devices without FIS-approved security precautions to prevent unauthorized access to that information.

Users are not permitted to "jailbreak" or change the operating system of any mobile device.

Personally-Owned Devices

Users must have FIS approval to use personally-owned devices to connect to University IT Resources. Users who choose to have FIS support a personally-owned device are subject to all applicable FIS policies, including but not limited to, the examination of personal data and the possible deletion of personal data on lost or stolen devices.

Privacy

Information stored on IT Resources is archived and stored for backup and recovery purposes. Thus, data, email, and other transactions may leave an audit trail or other record of the transaction, even when the data is later deleted or changed. For example, deleted data, email, network activity, and other transactions may have been archived and stored without any type of User action.

Upon appropriate authorization, FIS may search for, retrieve, and/or examine, data stored or transmitted to or from any IT Resource managed by FIS. This includes documents, data files, log files, and network/internet activity.

FIS does not engage in regular monitoring of IT Resources outside of performance tuning and maintenance. However, IT Resources may be audited or viewed by FIS without notice for work-related purposes or to prevent or investigate violations of these Guidelines, University policy, or applicable laws. Due to the need to protect the security of IT Resources, FIS cannot guarantee the privacy of information stored on any IT Resource.

Responsibility

The FIS Information Security Officer is responsible for overseeing all aspects of information security, including, but not limited to:

- Identifying, analyzing, and managing security risk and distributing information to appropriate personnel
- Identifying, analyzing, and ranking emerging security vulnerabilities
- Maintaining security incident response procedures
- Maintaining a formal security awareness program for all Users
- Creating and distributing security policies and procedures

Support

Users must submit all requests and incidents via the FIS Support Portal at www.fis.pitt.edu or through the FIS Support Hotline.

FIS considers any violation of these Guidelines to be a serious offense, and reserves the right to duplicate and examine any data or information resident on University IT Resources allegedly related to unacceptable use. Any IT Resource in violation of these Guidelines, or which poses a possible security risk, may be suspended or removed by FIS without notice. Any violation of the law involving IT Resources will also be considered a violation of these Guidelines. Departmental supervisors are responsible for ensuring Users in their area of responsibility are aware of these Guidelines.

Violations of these Guidelines may result in disciplinary action up to and including termination of employment as well as prosecution under applicable federal, state, and local laws.

Any reports of violations or questions about these Guidelines should be directed to:

John M. Duska
Executive Director, Technical Services
Information Security Officer
Financial Information Systems
jduska@cfo.pitt.edu

Monte A. Ciotto
Associate Vice Chancellor
Financial Information Systems
mciotto@cfo.pitt.edu