Information Technology Policy Common Definitions

Executive Summary

This document provides a common set of definitions for terms used in institute-level IT policies to ensure that common language and definitions are applied across these policies, standards, guidelines, and unit-level procedures.

Definitions

419 Scams: Named for the article of Nigerian law illegalizing the practice, these communications request assistance in collecting large sums of money by routing the money through the recipient’s bank account.

Application Server: The computer hosting the application that the general end-user or the point-of-sale (POS) terminal connects.

Availability: Time during which you can retrieve information when needed. Information can be unavailable due to destruction/erasure, system or network not working, or needed retrieval resources being overused.

Authorized Requesters: Unit heads or individuals with delegated authority to authorize and initiate access requests in accordance with established procedures by unit heads or higher-level management in their organizational reporting chain.

Authorized User (or Users): Georgia Tech employees or students who are authorized to access Institute Data in the performance of assigned duties.

Biometrics: The use of hardware and software to authenticate a person by measuring characteristics of their body, such as fingerprints, facial size and feature arrangement, handwriting style and speed, etc.
Blogs (or weblogs): Online web-based publications by individuals or small groups discussing daily occurrences or specific topics.

Cardholder Information Security Program (CISP): The formal data protection program mandated by Visa.

Card Verification Value 2 (CVV2): The verification code provided on some credit cards and required for some online transactions. Based on the requirements of multiple credit card companies, this information should not be stored beyond the time of the transaction.

Chief Data Stewards: Senior administrative officers of the Institute responsible for managing information resources while conducting Georgia Tech business. The Provost and Vice President for Academic Affairs and the Senior Vice President for Administration and Finance are Chief Data Stewards of Institute Data.

Computer & Network Usage and Security Policy (CNUSP): The GIT policy governing the behavior of students, employees, and others in the use of GIT information technology resources. Previously known as the CNUP (Computer & Network Usage Policy).

Confidentiality: Preventing the disclosure of information to any person not authorized to view, copy, or distribute that specific information.

Credit Card Database Servers: The computer storing the sales and/or credit card numbers.

Credit Card Number: Any part or all of the unique number identifying the account for a financial transaction.

Cryptography: The academic study of encryption.

Data Access Policy (DAP): The GIT policy established governing the categorization of data and the appropriate access controls required based on that categorization.

Data Administrator: Individuals responsible for documenting and enabling user access to a domain of Institute Data.

Data Categorization: The four categories of Institute Data defined in the Data Access Policy are:

- **Category I – Public Use:** This information is targeted for general public use. Examples include Internet website contents for general viewing and press releases.

- **Category II – Internal Use:** Information not generally available to parties outside the Georgia Tech community, such as directory listings, minutes from non-confidential meetings, and internal (Intranet) websites. Public disclosure of this information would cause minimal trouble or embarrassment to the Institute. This category should be the default data classification category.

- **Category III – Sensitive:** This information is considered private and should be guarded from disclosure; disclosure of this information may contribute to financial fraud and/or violate State and/or Federal law.

- **Category IV – Highly Sensitive:** Data which needs to be protected with the highest levels of security, as prescribed in contractual and/or legal specifications.

Data Coordinators: Individuals designated by the Data Stewards to coordinate data access for subsets of data, maintain records of authorized Data Users, and serve as contact points for the
Institute Data Administrator(s). Examples of "subsets of data" include Employee Data, Student Data, Auxiliary Services Data, Financial Data, and Sponsored Programs Data.

**Data Stewards:** Deans, Vice-Presidents, Associate Vice-Presidents, or others identified by the Chief Data Stewards to manage a subset of data (i.e., they are responsible for its accuracy, integrity, and implementation of policy and procedures for appropriate use of the data).

**Data Users:** Individuals who are authorized to access Institute Data in the performance of assigned duties, typically employees of the Institute or contractors.

**Data Views:** A logical collection of data elements, possibly from multiple physical databases, that are assembled and presented according to a defined set of rules.

**Denial of Service Attack (DoS):** A computer attack typically from a single system to take advantage of a remote system vulnerability to deny legitimate system or resource use.

**Digital Certificates:** A high-security form of authentication - the exchange of short, encrypted files by the programs that are communicating, which serve to authenticate the client and server processes to each other. There is an entire system of organizations and protocols that work together to create, authenticate, revoke, and use digital certificates. The user of a computer typically allows the program(s) to use digital certificates by logging in to the system or program with a user ID/password.

**Disaster Planning:** Creating, implementing, and testing plans and procedures for the continuation of essential business operations even after a disaster, such as an earthquake, hurricane, flood, extended power outage, terrorist incident, etc. Usually involves duplicated computing facilities, communications facilities, vendor agreements, employee procedures, etc.

**Distributed Denial-of-Service Attack (DDoS):** A computer attack by malicious code located on multiple systems where the intent is to overload the target computer(s) or network resources prevent legitimate system or resource use.

**eCommerce Application:** Any internet-enabled financial transaction application, whether a buying application or selling application.

**Employees:** Faculty (as defined by the Faculty Handbook), employees (as defined by the Classified Employee Handbook), visiting faculty from other educational institutes, guest lecturers, contractors, personnel from third parties on temporary assignment at GIT, and student employees.

**Encryption:** Using programs and measures to encode information such that it cannot be decoded and read without knowing an appropriate key – usually a user-selected key.

**Filtered:** The process of examining a file or content acquired through the network or from media (e.g. CD or diskette) for harmful or malicious content.

**Fingerprinting (of files):** Creating a mathematical summary of the file that is usually sufficient to detect any change to the file, but can be stored compactly (e.g. a hash or CRC of the entire file).

**Firewall:** A device or program designed to control the network traffic allowed to flow to a computer or segment of the network.
Hashing: Generating a unique value for a specific file, program, or communication that provides assurance that the information is complete and has not been tampered with. Part of the goal is providing enough of a signature to confirm that the information is complete without being able to generate the actual information from the hash.

Information Technology Resources: Computers, storage peripherals, network equipment and wiring, network-attached printers and fax machines.

Institute Data: Any data needed to conduct operations of the Institute.

Integrity: The amount of confidence that the information has not been modified in an unauthorized or incorrect way.

Intrusion Detection System (IDS): A network or workstation based system used to detect and notify critical individuals when an attack is launched.

Intrusion Prevention System (IPS): A network-based IDS that can automatically react and prevent attacks from successfully occurring. Special care must be taken with IPS to ensure that the system does not prevent communication that should occur, even during attacks.

Instant Messenger: A method for immediate communications between users

IP Spoofing: Providing a network address (IP address) that is not correctly assigned to purposely prevent others from locating the source for certain network traffic or messages.

ISO 17799: The International Standards Organization document defining computer security standards. The credit card vendors may have based their policies on this standard.

Keyboard Logging: Maintaining a file of the information input from the keyboard of a computer. This can be maintained on the computer or in a device attached to the keyboard.

LAWN: The Georgia Tech Local Area Wireless/Walkup Network. This authenticated network access provides wireless access to GIT and provides authentication for wired ports in some public areas.

Limited-access Room: A room that only a limited number of people possess keys to enter the room and authority to manage the IT equipment within the room.

Network Packet Capturing: Capturing information intended for others being transmitted across the network with the purpose of inappropriate examination later.

Newsgroups: Online discussion groups dedicated to specific topics

Payment Card Industry (PCI): A credit card industry standard (see also CISP and SDP).

Phishing: Sending spam noting an event requiring a person to provide personal information directly or go to a specially crafted website to provide personal information that is used for fraud.

Port Scanning: Using a program or manually examining all computer network ports (65,535 available) or a small subset on one or multiple computers.

POS Terminal: Point-of-sale (POS) computer terminals either running as standalone systems or connecting to a server either at the Georgia Institute of Technology or remotely off site.

Pre-logon banner: A message that is shown to the person attempting to login to a computer or communications facility BEFORE they are prompted to enter any authentication (user ID/password, biometrics, etc).
**Purchase Cards (P-Cards):** Credit cards obtained by Georgia Tech through a customer agreement with a bank for procurement purposes.

**Radio Frequency Allocation:** The assignment and management of radio frequencies or channels used by wireless networking transmission devices physically on Georgia Tech property (not currently leased to a third party), using Georgia Tech electricity, or connected to the Georgia Tech network. This currently includes channels in the 2.4 and 5 GHz frequency ranges.

**Senior Management:** The personnel designated by the unit head as the management team for a specific unit

**Sensitive Data:** Any information that requires special handling and safeguarding based on privacy, security, and/or legal requirements. Typically, this includes records containing any of the following data elements:
- Social Security Number
- Information protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Information protected by the Family Educational Rights & Privacy Act (FERPA)
- Institute financial records
- Personal information (beneficiary designation, financial aid application information)
- Passwords

**Site Data Protection Program (SDP):** The formal data protection program mandated by MasterCard.

**Social Engineering:** The collective term for many tactics used by people attempting to break security measures of an organization by working with employees’ desire to be helpful or their ignorance of proper security measures. An example would be an intruder posing on the phone as a new system administrator or auditor, who asks for your user ID/password “to check security on a system.”

**Spam (or unsolicited bulk e-mail – UBE, or unsolicited commercial e-mail – UCE):** E-mail distributed without (and frequently against) the recipient’s wishes to promote commercial offerings. This type of e-mail may represent 50%-70% of all e-mail on the internet in 2004.

**Spyware:** Software installed on a computer (typically from a website) to monitor and report computer use.

**Students:** Individuals enrolled at the Georgia Institute of Technology for academic pursuits.

**Swipe Terminal:** POS credit card terminals.

**Trojan Horse (program):** A program which consists of malicious code, but which is promoted as or appears to be a useful program, in order to trick an unsuspecting person into executing the program. This program would not be self-replicating and is normally targeted at an individual or system.

**Technical Authority:** Individual (internal or external to the unit) designated by unit head with the expertise to certify and sign-off on technical compliance with published standards of all workstations and servers used by the unit for accessing or storing Institute Data.

**Technical Lead:** The person designated by the unit head as the primary responsible party for information technology/information systems planning and implementation.
Technical Support Team: The group of people (where appropriate) handling information technology/information systems implementation and maintenance.

Two-factor Authentication: An authentication method requiring two items (beyond a user ID) for authentication. Typically, these items would be something you know (e.g. a password) and something you have (e.g. a number from a token, a fingerprint).

Unit: A fundamental workgroup identified in the official organizational chart of the Institute.

Unit Head: An individual responsible for direct oversight of a Unit.

Unit-level Servers: Servers that provide critical information services for department units, or ancillary systems that interface with centralized services, such as:

Web servers, fileservers, print servers, domain name servers, file transfer servers, firewalls, network storage devices, DHCP servers, unit-level remote access solutions and other ancillary systems

Virus: Malicious software that is executed by the user. The virus will spread to other computers and/or programs.

Voice over IP communications (VoIP): Telephone communications routed over a computer network using IP rather than a traditional telephone network.

Web Development: The design, development, implementation and management of front-end interfaces for web applications.

Wireless Access Point (AP): Any device providing connectivity from one computer or PDA to a network or other computer or PDA via radio frequency transmission.

Worm: A self-contained program that runs itself on a system which replicates to other systems without user intervention.

3. Definitions Modifications

These definitions may be revised by the responsible university officer to reflect the changing nature of technology and the changing regulatory landscape.