Glossary of Terms for Information Security

Term	Definition
Availability	Concerns the continued accessibility of information, systems and networks in order to meet institutional requirements.
CAB	Change Advisory Board – serves as the governing body for the review and approval of all changes to systems under management by ITS; operates under the auspices of the Chief Information Officer (CIO).
CAB Membership	Consists of ITS Managers reporting directly to the CIO, as well as other related technical positions. Membership is determined by the Chair.
Campus Network	Composed of all access layer switches, distribution and core routers, copper and fibre cabling that serves as the backbone network of the University.
Campus Network Infrastructure and Services	Includes the Campus Network and other supporting network infrastructure devices and systems, such as: DNS/DHCP, Firewall, VPN, Server Load Balancer, Wireless, Network Management System, Packet Shaper and Internet; and the corresponding services that it delivers to the University community.
Campus Wireless Network	Any public or private wireless network managed and configured by ITS.
Card Verification Data	The CVV (Card Verification Value) or CVN (Card Verification Number) or CID (Card Identification Number) is the three digit (or four digit on AmEx) security code that is printed on the back of a credit card. This number is never transferred during card swipes and should only be known by the cardholder (or the person holding the card in their hand).
Cardholder Name	Non-consumer or consumer customer to whom a payment card is issued to, or any individual authorized to use the payment card.
CDE	Cardholder Data Environment refers to the people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data.
CIO	Chief Information Officer.
Cloud Computing	A general term for anything that involves delivering hosted services; a type of computing where both applications and infrastructure capabilities are provided to end users as storing, processing and sharing information service through the Internet.
Confidential Data	A generalized term that typically represents data classified as confidential, according to the data classification scheme defined in this document. This term is often used interchangeably with sensitive data.
Confidential Information	Information to which access is restricted by law, policy, or practice; for example: personal information, third party commercial information or trade secrets, solicitor client privileged information, and research or teaching materials. Confidential information may include that which is not yet ready for public release such as drafts or not yet approved policy or planning documents.
Confidentiality	Concerns the safeguarding of information from unauthorized disclosure.
Custodian/Data Custodian	An employee of the University who has administrative and/or operational responsibility over information assets. May have physical custody of information; for example, third party data storage providers or paper record

	storage facilities. At Carleton, ITS has custody of Banner data but ITS is not the owner of Banner data.
Data Classification	In the context of information security, is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization.
Data Owner	Faculty, staff, students, visiting scholars, or researchers that have ownership of any data or information.
DHCP	Dynamic Host Configuration Protocol; a client/server protocol that automatically provides an IP address and other related configuration information such as the subnet mask and default gateway.
DNS	Domain Name Services; an Internet service used to resolve system names to network addresses and vice versa.
Electronic Commerce	Commonly known as e-commerce and consists of the buying and selling of products or services over electronic systems such as the internet.
Electronic Data	Information that is stored, transmitted, or read in an electronic format such as a file on a drive or device, or information in a database.
Encryption	Involves transforming information into an unintelligible format that can only be made legible using an authorized key or password.
Expiration Date	Date of expiry printed on the front of all credit cards.
Financial Information	Information about an individual's or an organization's financial matters, such as income, expenses, banking, and credit information.
Full Magnetic Stripe Data	May also be referred to as "full track data." Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic-stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe.
Hardcopy Data	Information that is stored and read in a physical format such as a paper file or a book.
Harm	Anything that has a negative effect on the welfare of an individual or organization; the nature of the harm may be social, behavioural, psychological, physical, or financial.
Identifiable Individual	An individual who could reasonably be identified, directly or indirectly through personal information; or an individual who can be reasonably identified by linking separate groups of information.
Information	A collection of data, regardless of format or carrier medium, that may or may not be aggregated into a record.
Integrity	Concerns the protection of information from unauthorized, unanticipated or unintentional modification; including accidental deletion in whole or in part.
Internal Data	All data owned or licensed by the University.
ITS	Information Technology Services.
Non-public Information	Any information that is classified as Internal or Confidential Information according to the data classification scheme defined in this document.
Operational Security Controls	Procedural, organizational, or personnel security safeguards. Examples of operational security controls would be the use of reference checks to validate the experience of a job applicant or the assessment of systems for compliance with privacy protection legislation.
Owner	Responsible for the management of the business processes whereby

	records and the information they contain are created, used or accessed.
PCI DSS	Payment Card Industry Data Security Standard is a standard developed by the PCI Security Standards Council to protect against fraud in credit card transactions.
Personal Health Information (PHI)	Information about an identifiable individual and related to their health or health care history including but not limited to medical history, details or visits to health-care practitioners, and test results.
Personal Identification Number (PIN)	Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system.
PIN Block	A block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed to retrieve the PIN. The PIN block is composed of the PIN, the PIN length, and may contain a subset of the PAN.
Personal Information/ Personally Identifiable Information	Recorded information about an identifiable individual including but not limited to the individual's name, age, race, sex, address, SIN, or other identifying numbers, financial history, education, and/or employment history, personal opinions, and more. Personal information ranges in sensitivity, becoming more sensitive in accordance with the risk and/or harm that may ensue as a result of unauthorized release or disclosure of the information.
Physical Security Controls	Facility and environmental safeguards used to protect information and systems. A secure environment that is not accessible to the public. The location can be secured by a lock and access limited to authorized individuals. An example of a physical security control would be a combination lock on the door to a server room as well as locked cabinets, drawers or other locked, coded or password protected devices.
Primary Account Number (PAN)	Unique payment card number that identifies the issuer and the particular cardholder account.
Point of Sale (POS) Terminal	Hardware and/or software used to process payment card transactions at merchant locations.
Proprietary Information	Information that is exclusive to the owner with all the rights that the owner can exercise. Proprietary information is not necessarily confidential.
Record	Information arranged in the context required to document institutional processes for evidentiary, legal and historical requirements.
Research Data/ Information	Information collected, obtained, and used during the course of research. Includes original data, previously existing data sets (secondary use), as well as the analysis, results, or dissemination resulting from the research process.
RF Band	Radio frequency band.
Security	Enables the protection of assets or property, including information or data, through the application of physical, technical, and/or administrative safeguards.
Sensitive Data/ Information	Includes but is not limited to personally identifiable information, and must be defined according to context and the expectation of the individual or entity to whom the information relates. For example, the names and addresses of subscribers to a University mailing list would generally not be

	considered sensitive information. However, the names and addresses of subscribers to a specific research interest group may be considered sensitive. Federal and provincial legislation, as well as contractual obligations and agreements may also specify data elements that require protection from unauthorized creation, access, modification and/or deletion.
Service Code	Three- or four-digit value in the magnetic stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.
Technical Security Controls	Safeguards implemented on IT systems to maintain confidentiality, integrity, and/or availability of the systems and data. An example of a technical security safeguard would be the use of a firewall to protect internal networks from the Internet.
TLSP	Transport Layer Security Protocol; cryptographic protocol designed to provide communications security over a computer network.
User	Does not create or control the use of, or access to, information or systems, but has the use of, or access to, information in compliance with established policy. For example, access to Banner data according to job function.
Valid Business Purpose	Documents should be kept for six months in order to respond to disputes. This is a function of our relationship with respect to chargebacks and ChasePaymentech. This is not the same as the seven-year document retention requirement for Canada Revenue Agency audit purposes.
VPN	Virtual Private Network extends a private network across a public network, such as the Internet. Enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.