Carleton College

Data Risk Classification Guidelines

Carleton College is committed to protecting the privacy of its students, alumni, parents, faculty, staff, and all affiliated entries, as well as protecting the confidentiality, integrity and availability of information important to the College's mission.

Carleton has classified its information assets into risk based categories for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect it against unauthorized access.

As of August 2016, a new set of classification guidelines has been established and is now in effect for Carleton College data and systems: **Low Risk, Medium Risk,** and **High Risk.** The former data management framework of "Protected, Sensitive and Public" has been replaced by these new guidelines[1].

> Special note to Carleton researchers: Except for regulated data such as Protected Health Information (PHI), Social Security Numbers, and financial account numbers, research data and systems predominately fall into the Low Risk classification. Review the classification definitions and examples below to determine the appropriate risk level to apply.

Low Risk

Data and systems are classified as Low Risk if they are not considered to be Medium or High Risk, and:

1. The data is intended for public disclosure, or
2. The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on our mission, safety, finances or reputation.

Medium Risk

Data systems are classified as Medium Risk if they are not considered to be High Risk, and:

1. The data is not generally available to the public or
2. The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on our mission, safety, finances or reputation.

High Risk

Data and systems are classified as High Risk if:

1. Protection of the data is required by law/regulation
2. Carleton is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed, or
3. The loss of confidentiality, integrity, or availability of the data or system could create a significant adverse impact on our mission safety, finances or reputation.

[1] Training and document transition will be completed over the next twelve to eighteen months with direction and support provided by Carleton Information Technology Services (ITS) and Department File Management Stewards.

Carleton College

Data Risk Classification Examples

Use the examples below to determine which risk classification is appropriate for a particular type of data. When mixed data falls into multiple risk categories, use the highest risk classification across all.

Low Risk

- Research data (at data owner's discretion)
- Carleton Network ID's
- Information authorized to be available on or through Carleton's website without Carleton Network ID authentication
- Policy and procedure manuals
- Job postings
- College contact information in the Carleton Directory
- Information in the public domain
- Publicly available campus maps

Medium Risk

- Unpublished research data (at data owner's discretion)
- Student records and admission applications
- Grades and other student work product
- Faculty/staff employment applications, personnel files, benefits, salary, birth date, personal contact information
- Non-public Carleton policies and policy manuals
- Non-public contracts
- Carleton internal memos and email, non-public reports, budgets, plans, financial information
- College and employee ID numbers
- Project/task/award (PTA) numbers
- Engineering design and operational information regarding Carleton infrastructure
- Licensed software & software license keys

High Risk

- Health information, including Protected Health Information (PHI)
- Health Insurance policy ID numbers
- Social Security Numbers
- Credit card numbers
- Financial account numbers
- Information covered by U.S. export laws
- Driver's license numbers
- Passport and Visa numbers
- Donor contact information and non-public gift information
- Passwords and Security keys

Carleton College

Application Risk Classification Examples

An application is defined as software running on a server that is network accessible and that stores, processes or transmits College data. When mixed data falls into multiple risk categories, use the highest risk classification across all.

Low Risk

- Applications handling Low Risk Data
- Online maps
- College online catalog displaying academic course descriptions
- Bus schedules

Medium Risk

- Applications handling Medium Risk Data
- Human Resources application that stores salary information
- Directory containing phone numbers, email addresses, and titles
- College application that distributes information in the event of a campus emergency
- Online application for student admission

High Risk

- Applications handling High Risk Data
- Human Resources application that stores employee SSNs
- Application that stores campus network node information
- Application collecting personal information of donor, alumnus, or other individual
- Application that processes credit card payments
- Passwords

Carleton College

Server Risk Classification Examples

A server is defined as a host that provides a network accessible service. When mixed data falls into multiple risk categories, use the highest risk classification across all.

Low Risk

- Servers used for research computing purposes that do not involve Medium or High risk data
- Servers with potentially lower response time for parts replacement
- For example: File server used to store published public data, database server containing Network ID's only

Medium Risk

- Servers handling Medium Risk Data
- Servers with industry standard practices for patching and monitoring
- For example: for systems that store student records, salary and other financial information and non-public College contracts

High Risk

- Servers handling High Risk Data
- Servers with the highest level of restricted access, fail-over and monitoring
- For example: for hosting College email systems, Active Directory and Domain Name Server (DNS)

End-Point Risk Classification Examples

An end-point computer is a device that community members use to access College data. When mixed data falls into multiple risk categories, use the highest risk classification across all.

Low Risk

- End-point computers in public / shared locations
- Unprotected mobile devices
- College-owned and personally-owned computers

Medium Risk

- Encrypted or unencrypted desktop or laptop computers
- Mobile devices with pin code (and two-factor)
- College-owned computers and fully patched and protected personal computers.

High Risk

- Encrypted desktop or laptop computers
- End-point computers with login password and auto-screen lock
- College-owned computers (i.e. high risk data should not be synced to personal computers).

Carleton College

Existing Services

This chart is intended to be a general guide to direct users to appropriate data storage solutions. The list does not include all campus applications nor does it provide all information needed to store data in these applications securely. A procedural document is available from Information Technology Service (ITS)[2].

If your service is not listed consider it available for LOW RISK data only.

In addition to the services detailed below, Carleton College contracts for storage of medium to high risk data in specialized third party products such as Colleague, Slate and Advance.

	LOW RISK	MEDIUM RISK	HIGH RISK
Communication: Email and Voicemail	✓	✓	*
Carleton Dropbox and Google Drive: Narrowly Shared	✓	✓	*
Carleton Dropbox and Google Drive: Links	✓	*	
Non-Carleton Dropbox, Google Drive, iCloud, etc.	*		
Document Management: OnBase	✓	✓	*
Document Management: Protected Drive	*	✓	✓
Content Management: Reason	✓	✓	
Content Management: Word Press	✓	✓	
Content Management: Confluence/Carlpedia	✓	✓	
Content Management: Content Data Mart	✓		
Document Management: Home Drive	✓		
Document Management: Hard Drive on your computer	✓		
Document Management: thumb drive (portable storage device)	✓		
Organization: Google Sites	✓		
Survey Management: Qualtrics	✓	[3]	
US Postal Service and other mail services	✓	✓	✓
File Cabinets (unlocked)	✓		
File Cabinets (locked)	✓	✓	✓

[2] The ITS document of procedures for storing digital data securely is available via the ITS Service Catalog. The cells in this chart containing the * symbol are explained more fully in that procedure document.

[3] The Carleton Institutional Review Board (IRB) is a necessary partner for human subject surveys and the defining of appropriate gathering and sharing of such data.

Carleton College

Definitions

Computing Equipment

Any Carleton or non-Carleton desktop or portable device or system

Masked number

(i) A credit card primary account number (PAN) has no more than the first six and the last four digits intact, and (ii) all other Prohibited or Restricted numbers have only the last four intact.

NIST-Approved Encryption

The National Institute of Standards and Technology (NIST), develops and promotes cryptographic standards that enable U.S. Government agencies and others to select cryptographic security functionality for protecting their data. Encryption which meets NIST-approved standards is suitable for use to protect Carleton's data if the encryption keys are properly managed. In particular, secret cryptographic keys must not be stored or transmitted along with the data they protect. Cryptographic keys have the same data classification as the most sensitive data they protect.

Payment Card Industry Data Security Standards

The practices used by the credit card industry to protect cardholder data. The Payment Card Industry Data Security Standards (PCI DSS) comprise an effective and appropriate security program for systems that process store, or have access to Carleton's Prohibited or Restricted data. The most recent version of the PCI DSS is available here https://www.pcisecuritystandards.org/pci_security/

Protected Health Information (PHI)

All individually identifiable information that relates to the health or health care of an individual and is protected under federal or state law. For questions about whether information is considered to be PHI, contact the College's HIPAA Officer.

Qualified Machine

A computing device located in a secure Carleton facility and with access control protections that meet current Payment Card Industry Data Security Standards.

Student Records

Information required to be maintained as non-public by the Family Educational Rights and Privacy Act (FERPA) Student Records include Carleton-help student transcripts (official and unofficial), and Carleton-held records related to (i) academic advising (ii) health/disability, (III) academic probation and/or suspension, (iv) conduct (including disciplinary actions), and (v) directory information maintained by the Office of the Registrar and requested to be kept confidential by the student. Application for student admission are not considered to be Student Records unless and until the student attends Carleton.

Carleton College

Who do I contact for questions?

General Questions

Data	Responsible Office	Help
FERPA Compliance Student Records	Registrar	Submit help request https://apps.carleton.edu/campus/registrar/
Employee Records, including PHI	Human Resources	https://apps.carleton.edu/campus/human_resources/
PCI-DSS (credit cards)	Business Office	https://apps.carleton.edu/campus/business/
PHI (health info)	Student Health & Counseling	https://apps.carleton.edu/studenthealth/
Title IX Records	Title IX Coordinator	https://apps.carleton.edu/dos/sexual_misconduct/title_ix/
Research Subject Data	Institutional Review Board	https://apps.carleton.edu/governance/institutional_review_board/Info/
Other	CTO or Information Security Officer	https://apps.carleton.edu/campus/its/

Suspected Information Security Incident

Business Unit	Website	Help
Information Technology Services	https://apps.carleton.edu/campus/its/	X 5999 or helpdesk@carleton.edu

Report Lost or Stolen Device

Business Unit	Website	Help
Information Security Officer	https://apps.carleton.edu/campus/its/	X 5999 or helpdesk@carleton.edu
Campus Security	https://apps.carleton.edu/campus/security/	X 4444