	TASK	PUBLIC	INTERNAL	CONFIDENTIAL
UNDERSTANDING	Identify the Data Owner	All data must have or be assigned a Data Owner, who is overall responsible for the collection of the data as well as assigning the data classification and user roles including data users, data custodian and technical owners (which can be one or several persons for various roles).		
	Risk Level Assessment	Data owner(s) must assess the level of risk, according to the magnitude of harm and the probability of occurrence, should the data be compromised (lost, stolen or accessed by unauthorized parties).		
	Data Classification	Based on the Risk Level Assessment, the data owner(s) must assign a data classification in accordance to the University's Data Classification Policy.		
CREATING	Data on physical documents	No specific requirements	Data must be created securely; be aware of who has access to the data as it is being written or collected (by all senses as applicable - ear, sight, smell touch or taste).	
	Data on personal computers			
	Data on mobile devices (smart phones, tablets)			
	Data on Portable Media			
	Data on University workstation			
	Data on servers hosted at Carleton	Server(s) must be appropriately configured, hardened and patched.	Data must be created securely; be aware of who has access to the data as it is being written or collected (by all senses as applicable - ear, sight, smell touch or taste). Additionally, server(s) must be appropriately configured, hardened and patched.	
	Data created via remote connection (not local to Carleton University network)	Communications must be secure (HTTPS).	Data must be created securely; be aware of who has access to the data as it is being written or collected (by all senses as applicable - ear, sight, smell touch or taste). Additionally, communications must be secure (HTTPS).	
	Data on servers not hosted at Carleton (cloud services, online surveys, collaboration solutions)	Communications must be secure (HTTPS) and subject to approval from an Information Security Assessment.	Data must be created securely; be aware of who has access to the data as it is being written or collected (by all senses as applicable - ear, sight, smell touch or taste). Additionally, communications must be secure (HTTPS) and subject to approval from an Information Security Assessment.	

STORING	Data on physical documents	No specific requirements	Stored in secured location when not in use; filing cabinet with access control implemented (lock and key). Shared with internal persons and limited external persons.	Stored in secured location when not in use with data classification label displayed; fireproof cabinet with access control implemented (lock and key). Shared on a need to know basis only.
	Data on mobile devices (smart phones, tablets)	No specific requirements	Physically store equipment in a secure location when not in use. Mobile devices should have Carleton University's MDM software installed. Portable media must have data and /or disk encryption.	
	Data on Portable Media			
	Data on personal computers	No specific requirements	Physically store equipment in a secure location when not in use. Avoid saving data locally. Permitted only if joined to the Carleton University CUNET domain. If not joined to CUNET, encryption is required.	
	Data on University workstation			
	Data on servers hosted at Carleton	Servers hosting data must be appropriately configured, patched and security hardened with controlled access. Encryption not required.		
	Data on servers not hosted at Carleton (cloud services, online surveys, collaboration solutions)	Subject to approval following an Information Security Assessment and a Privacy Impact Assessment. Communications must be secure (HTTPS). Payment data must be encrypted or obfuscated. Transactional data should not be stored (See eCommerce Policy).		
USING	Adhere to Acceptable Use Policy for Information Technology (IT)	No specific requirements	Be aware of individuals who are not authorized to view the information; documents in plain view or left unattended where unauthorized personnel can gain access. Adhere to safe computing practices; avoid unnecessary screen sharing, shoulder surfing and leaving active login sessions unattended (unlocked).	
	Copying /duplicating documents	No specific requirements	As far as reasonably possible, data classification must be labelled or notification displayed. See Storage for additional requirements.	
	Printing (hard copy) data	No specific requirements	Unattended printing permitted only if physical access controls are in place to prevent unauthorized viewing.	
	Auditing and Logging	Audit access processes periodically, referring to the data classification process for guidance as needed.	Logging should be enabled as defined by policy or business requirements. Audit access processes periodically, referring to the data classification process for guidance as needed. System Custodians shall review all access violation attempts and notify Data Steward and/or Information Security Office of any suspicious or abnormal activity.	

SHARING	Traditional Mail (Campus mail, Canada Post or Courier)	No specific requirements	Confidential data must be placed into a sealed package and labelled "Confidential". This must then be placed into another package. Internal data must be placed into a sealed package. Outer packaging that does not leave campus can be labelled accordingly. If recipient(s) delivery address is external to campus then outer packaging must not be labelled. As far as reasonably possible, Confidential package(s) should be hand delivered.
	Carleton University Email	No specific requirements	Label as "Internal" or "Confidential" in the subject line accordingly. Confidential data (content of email and/or attachment) must be encrypted or obfuscated, without password included.
	Personal Email	No specific requirements	Not Permitted
	Social Media		
	Granting permission to view, create or modify data	No specific requirements	Access is restricted using various access control methods and is based on roles, classes, entitlements, or affiliations defined by respective Data Owner or the designate Data Steward. Refer to FIPPA (Freedom of Information and Protection of Privacy)
	Granting permission to delete data	No specific requirements	Deletions are restricted using various access control methods and are based on roles, classes, entitlements, or affiliations defined by respective Data Owner or the designate Data Steward. Also adhere to records management requirements for deleting data (Corporate Records and Archives Policy).
	Sharing data	No specific requirements	Create a Data Sharing Agreement with third parties that will be receiving the data. For more information, contact its-secops@carleton.ca. Label documents with data classification as well as type (Duplicate or Original). Adhere to mail requirements outlined above. External users must comply with data treatment standards.
ARCHIVING	Adherence to Archival processes	Please see Corporate Records and Archives Policy	
	Adherence to Storing requirements	Archived data in any format must first comply with the Storing requirements (See above section).	
	Physical data stored on Carleton University premises	No specific requirements	Physical files and documents must be stored in an area with physical access controls and appropriate fire protection systems.
	Physical data stored at external third party premises	No specific requirements	Physical files and documents must be stored in an area with appropriate fire protection systems and physical access controls that limit third party from having unrestricted access.
	Electronic data stored on devices physically located on Carleton University premises (portable media, mobile devices, servers, workstations)	No specific requirements	Electronic data must be encrypted when stored at rest, in an area with physical access controls and suitable fire protection systems.

	Electronic data stored on devices not physically located on Carleton University premises (portable media, mobile devices, servers, cloud, personal computers)	No specific requirements	Electronic data must be encrypted when stored at rest, in an area with suitable fire protection systems and access controls that limit third party from having unrestricted physical and logical access.
DESTROYING	Disposing of physical data files and folders	Adhere to retention schedules. For more information refer to Corporate Records and Archives Policy.	
	Disposing of data (e.g., legacy data, archived data, expired or unneeded data, etc.)	Adhere to retention schedules. Manually or automatically attempt to verify that Confidential data has been removed. The data must be digitally shredded and /or storage device low level formatted, not just deleted. Please refer to IT Disposal Guidelines and Best Practices: http://www.carleton.ca/its/we_need_disposal_guidelines.html For more information refer to Corporate Records and Archives Policy	
	Disposing of surplus physical electronic media device (e.g. disks, hard drives, CDs, backup tapes and other portable media)	Media must be securely destroyed in accordance with the IT Disposal Guidelines and Best Practices. Please refer to: http://www.carleton.ca/its/we_need_disposal_guidelines.html	