CP 6-9f: Data Storage

COLLEGE PROCEDURE: CP 6-9f
APPROVED: November 02, 2021
EFFECTIVE: November 02, 2021
REFERENCES: N/A

Procedure summary

Users of Dawson Community College (DCC) IT resources shall store data in designated, secured, recoverable, and administered data repositories.
This Procedure shall be subject to and superseded by applicable regulations and laws.

Scope statement

This Procedure applies to all data for which DCC is custodian. Impacted personnel are all staff, faculty, students, and any third party using DCC data.

Statement of purpose

DCC's Information Security Policies support the following goals:

1. Promote a "security is everyone's responsibility" philosophy to assist DCC in meeting its business and legal commitments.
2. Ensure that DCC complies with all applicable laws and regulations.
3. Ensure the integrity, reliability, availability, and superior performance of IT resources.
4. Ensure that users are protected from data breach and cybercrime.
5. Ensure that use of IT resources is consistent with the principles and values that govern the use of other college facilities and services.
6. Prevent unauthorized disclosure of controlled sensitive data.
7. Prevent disruption of the learning experience.
8. Ensure the college is protected from financial, legal, regulatory, and reputational harm.
9. Ensure that IT systems are used for their intended purposes.
10. Establish processes for addressing Procedure violations and sanctions for violators.

DCC has a duty to protect, administer, backup, and recover data for which we are custodian. This can only be achieved with the cooperation of the users of the data. When data is not stored in officially designated systems and repositories, DCC does not have the capability to fulfill its regulatory and operational responsibilities.
In addition, DCC data repositories should only be used for their intended purpose. Storing unnecessary data (such as personal files) creates additional unnecessary operational and regulatory risk. Unfortunately, achieving this is often a trade-off between convenience/expediency and best practice. While appropriate training can raise awareness of these issues, it is the duty of every user of DCC data to understand the implications of their actions with respect to how they manage data.

Procedure

1. Only data and files that are related to DCC pedagogical, business, and operational activities shall be stored in DCC data repositories.
2. Users shall use their individual Google Drive to store data.
3. Users shall not store data on local computer hard drives (e.g. "CDrive"), unencrypted personal USB drives, personal Cloud storage, or mobile devices.

4. Departmental data shall be stored on departmental shared drives (e.g. H:Drive) or Google Drive.
5. Data shall be archived after one year of inactivity.
6. Archived electronic data shall be removed from DCC's systems on a schedule defined by DCC's Business Data Retention Procedure.

Exemptions

Data may be stored in the DCC "Spaces" wiki as appropriate for communication, collaboration, and reference. It is not recommended that "Spaces" be used as a departmental or general data repository. Controlled sensitive data shall not be stored in Spaces.

Procedure violation

1. Violation of this Procedure may result in disciplinary action in accordance with DCC Human Resources and/or Student Conduct guidelines.
2. DCC reserves the right to report security violations or compromises to the appropriate authorities. This may include reporting violations of Federal, State, and local laws and regulations governing computer and network use, or required accreditation reporting.
3. Anyone who violates this Procedure may be held liable for damages to DCC assets, including but not limited to the loss of information, computer software and hardware, lost revenue due to disruption of normal business activities or system down time, and fines and judgments imposed as a direct result of the violation.
4. DCC reserves the right to deactivate any User's access rights (whether or not the User is suspected of any violation of this Procedure) when necessary to preserve the integrity of IT Resources.

Complaint procedures

Report non-security-related violations (such as receipt of inappropriate content, other Human Resource Procedure violations, general college Procedure violations, or regulatory compliance violations) to a supervisor, HR, or EthicPoint.
Report information security and general technical Procedure violations to the IT Service Desk at 971-722-4400 or servicedesk@DCC.edu.

Definitions

- Cloud Computing
  A general term for the delivery of hosted computing services over the internet.
  - Cloud computing enables companies to consume a compute resource, such as a virtual machine (VM), storage, or an application, as a utility service.
  - DCC's Google "G-Suite" environment (that supports Gmail, Google Drive, etc.) is a Cloud service. The students' PantherHub is another example of Cloud technology.
- Controlled Sensitive Data (CSD)
  A general categorization that is used in DCC's Information Technology (IT) policies (primarily the Information Security Procedure and the Acceptable Use Procedure) to represent all confidential and private information governed by those policies.

- CSD includes: PII, PHI, HIPAA, FERPA, regulated, private, personal, or sensitive information for which DCC is liable if publicly disclosed.

- Cybercrime
  Criminal activity or a crime that involves the Internet, a computer system, or computer technology.
- Data Breach
  Generally, an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so.
  - Note: Although "breach" is a commonly used term in the information security community, legally, the term "breach" tends to only be used when a security event reaches the threshold of regulatory reporting. DCC legal council recommends using the terms "incident" or "compromise" until it can be determined whether an event satisfies the legal definition of a breach.
- Encryption
  The process of converting data to an unrecognizable or "encrypted" form.
  - Encryption is commonly used to protect sensitive information so that only authorized parties can view it.
- Hard Disk
  A data storage device that uses magnetic storage to store and retrieve digital information using one or more rigid, rapidly rotating disks (platters) coated with magnetic material.
- Hardware
  The collection of physical components that constitute a computer system (a desktop computer, a server in a datacenter, a network switch, a printer, etc.)
- IT Resource
  (At DCC) All Information Technology (IT) resources that are the property of DCC and include, but are not limited to, all network-related systems; business applications; network and application accounts; administrative, academic and library computing facilities; college-wide data, video and voice networks; electronic mail; video and web conferencing systems; access to the Internet; voicemail, fax machines and photocopiers; classroom audio/video; computer equipment; software and operating systems; storage media; Intranet, VPN, and FTP.
  - IT Resources include resources administered by IT, as well as those administered by individual departments, college laboratories, and other college-based entities.
- Software
  A set of instructions that tells a computer what to do.
  - Computer software is generally constructed as programs (applications) written in a specific language designed to run
    on computer hardware. Most common softwares are applications for business and personal use. More specialized computer software runs the operating systems of computers, operates machinery, creates artificial intelligence in robots, controls scientific instruments, etc.
- System
  (In Information Technology [IT]) A computer system consists of hardware components that work with software components to achieve a defined outcome.
  - The main software component that runs on a system is an operating system that manages and provides services to other programs that can be run in the computer. Computer systems may also include peripheral devices such as printers, A/V equipment, operating machinery, etc.
- USB "Thumb" Drive
  A portable data storage device that includes flash memory. Has a USB connector that plugs into the USB socket on a computer.
- User

Any person who makes any use of any DCC IT resource from any location (whether authorized or not).

SCOPE This Procedure applies to Dawson Community College.

PROCEDURES The College President shall promulgate such procedures as may be needed to implement this Procedure.

History: 11/02/2021