CP 6-9A: Data and Retention and Disposal

COLLEGE PROCEDURE: CP 6-9A

APPROVED: November 02, 2021
EFFECTIVE: November 02, 2021
REFERENCES: N/A

Procedure summary

Regardless of storage location, all controlled sensitive data shall be securely retained only as long as required for legal, regulatory, and business requirements.
This policy shall be subject to and superseded by applicable regulations and laws.

Scope statement

All Dawson Community College (DCC) employees, students, and affiliates or other third parties that create, use, maintain, or handle DCC IT resources are subject to this policy. This policy applies all controlled sensitive data stored using DCC IT Resources.

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 policy violations and sanctions for violators.

DCC is subject to regulations that require the retention and availability of certain data. Best practice is that data is retained for the period required for compliance. However, college leadership my request certain data be retained for longer periods or indefinitely.
This is both an operational and information security issue for IT. From an information security perspective, retained data must continue to be stored securely – even if not actively used. This may require different techniques than normal operations, as the data may be archived, or otherwise maintained differently, from active data. In addition, data retained beyond the required period represents unnecessary information security risk (i.e. a breach of archived data has the same implications to the college as a breach of active data).

Policy

1. The data owner shall establish the regulatory retention length in accordance with state and federal laws, or other regulations governing a public institution.

2. If data retention requirements are not explicitly documented, IT shall retain data indefinitely.
3. All controlled sensitive data that has passed its required retention shall be deleted from DCC electronic storage.
4. All hardcopy controlled sensitive data that has passed its required retention shall be disposed of in a secure way.
5. Media containing controlled sensitive data that has passed its required retention shall be disposed of in a secure and safe manner, using industry best practices.
6. Outsourced destruction of media containing controlled sensitive data shall use a bonded disposal vendor that provides a "certificate of destruction."
7. Controlled sensitive data shall be deleted from copying and communications equipment before such equipment is provided to any vendor for trade-in, servicing, or disposal.
8. DCC shall randomly sample sanitized media to ensure proper destruction.

Exemptions

Data owners, with Cabinet approval, may request extension of retention periods beyond compliance requirements.

Policy violation

1. Violation of this policy 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 policy 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 policy) 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 policy violations, general college policy violations, or regulatory compliance violations) to a supervisor, HR, or EthicPoint.
Report information security and general technical policy violations to the IT Service Desk at 971-722-4400 or servicedesk@DCC.edu.

Definitions

- Binary Wipe
  A process that permanently deletes all data from an electronic storage medium, such that it cannot be recovered.
- Chief Information Security Officer (CISO)
  Senior manager responsible for information security compliance at DCC.

- Compact Disk (CD)
  A small plastic disc on which music or other digital information is stored, and from which the information can be read using reflected laser light. Because of the use of light, CDs are a type of data storage media referred to as Optical Storage.
- Controlled Sensitive Data (CSD)
  A general categorization that is used in DCC's Information Technology (IT) policies (primarily the Information Security Policy and the Acceptable Use Policy) 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.
- DVD
  A type of compact disk able to store large amounts of data, especially high-resolution audiovisual material.
- 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.
- Degauss
  A way of wiping electronic data storage media so that it is no longer usable and data cannot be
  - accessed.
    Degaussing works by eliminating remnant magnetic field.
- 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.
- Hardcopy
  A printed version on paper of data held in a computer.
- 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.
- Optical Disk
  A common form of electronic media technology (e.g. CD, DVD).
  - A flat, usually circular disc which encodes binary data (bits) in the form of pits (binary value of 0 or off, due to lack of reflection when read) and lands (binary value of 1 or on, due to a reflection when read) on a special material (often aluminum) on one of its flat surfaces.
- Platter
  Also known as hard disk, the circular disk on which magnetic data is stored in a hard disk drive.
- 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.

SCOPE This Policy applies to Dawson Community College.

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

History: 11/02/2021