CP 6-8e: Data Classification and Control

COLLEGE PROCEDURE: CP 6-9e

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

Procedure summary

All data stored and accessed on DCC information systems, whether managed by employees or a third party, shall be identified and classified by the data owner in collaboration with the data custodian. The classification level of the data shall be reviewed on a periodic basis, as applicable to current state and federal laws and regulations, and periodic reviews of user access shall be performed.
This Procedure shall be subject to and superseded by applicable regulations and laws.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 Procedure. This Procedure applies all controlled sensitive data stored or transmitted using DCC IT Resources and all users of such 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.

This Procedure supports the primary goal of regulatory compliance, which is to protect critical data such as student PII and other sensitive information. In order to do this, the data stored in DCC systems must be understood and appropriate controls (whether digital or physical) implemented to appropriately protect data from breach and manage access to the data. This Procedure seeks to ensure that DCC takes all necessary steps to meet regulatory compliance standards in respect to classifying and controlling critical data.

Procedure

1. All controlled sensitive data shall be protected via access controls to ensure data is not improperly disclosed, modified, deleted, or rendered unavailable.
2. Users shall be granted access to DCC systems based on role. Users shall be given enough access to view and update information as required to accomplish their jobs and no more.

3. All hardcopy materials and stationary electronic media containing confidential and/or sensitive information shall be protected by appropriate physical access controls.
4. Appropriate facility controls shall be used to limit and monitor individual physical access to systems that store controlled sensitive data. Facility controls shall include alarm procedures, user authorization (e.g., card access), coverage requirements, escalation procedures, and testing procedures.
5. Visitor logs and physical audit trails of access to controlled sensitive data by individuals who do not own the data shall be collected and retained for a minimum of three months, unless otherwise restricted by law.
6. The CISO shall perform a bi-annual audit of computer resource authorizations to confirm access privileges are appropriate. The audit will consist of validating access rights for sample user populations.
7. Extensions for affiliate accounts shall be authorized by the CISO to provide an audit trail.

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

- Access Control
  The selective restriction of access to a place or computing resource for security purposes.
  - The act of accessing may mean consuming, entering, or using. For example, the lock on your front door is an access
    control mechanism to limit who can enter your house. Similarly, entering a user ID and password restricts access to your computer account.
- Affiliate
  Any person or entity that has been sponsored by a DCC manager to receive controlled temporary access to DCC services.

- This is generally as a result of a contractual relationship with DCC. For example, an air conditioning vendor may require affiliate access to test the HVAC system. A consultant project manager may require affiliate access to access project plans on a DCC system.

- Authorization

  Permission to access a specific piece of data or system function is called authorization.
  - A common form of authorization is "role-based" – a system may look up the role assigned to a particular user and only grant that user access to the functions of a computer program that are authorized for that role. For example, users associated with the "Payroll Administrator" role in Banner can access the payroll functions that they need to perform their job, but other Banner users cannot.
- Automatic Clearing House (ACH)

  An electronic network for financial transactions in the United States.
  - ACH allows DCC to execute electronic financial transactions with other financial institutions. ACH credit transfers include direct deposit, payroll, and vendor payments.
- Chief Information Officer (CIO)

  Senior manager of the Information Technology (IT) Department and a member of Cabinet.
  - At DCC, the CIO is responsible for all technology, with the exception of:
    - Online Learning (Academic Affairs)
    - Some specialized technology that supports CTE or other engineering programs (e.g. software that supports machine labs, specialized dental technology, etc.)
    - Some technology that supports auxiliary services (e.g. Point of Sale systems in the cafeterias and bookstores)
- Chief Information Security Officer (CISO)

  Senior manager responsible for information security compliance at DCC.
- 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.
- Electronic Media

  Technology that stores and accesses data in electronic form.
  - In contrast to static media (e.g. print media). Digital Content is stored on Electronic Media.
- 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.
- Information Security Manager (ISM)

  (aka Associate CISO) Manager of the DCC Information Security team, reporting to the CIO and/or CISO.
- Personally Identifiable Information (PII)

Any data or combination of data that could potentially identify a specific individual.
  - Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.
- 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.
- Third Party
  (In Information Technology [IT]) A vendor. Can be applied to any vendor ("third party provider"), but mostly used regarding "vendor software" to distinguish it from software developed "in house."
- 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