

## CP 6-9g: Employee Identification

---

### COLLEGE PROCEDURE: CP 6-9g

APPROVED: November 02, 2021

EFFECTIVE: November 02, 2021

REFERENCES: N/A

---

### Procedure summary

Employees, contractors, affiliates, or any other person entering Dawson Community College (DCC) facilities shall use their DCC-approved physical access mechanisms to gain physical access to secure facilities. Visitors shall not access DCC secure facilities unless access has been explicitly granted by a DCC employee or they have been assigned a physical access mechanism by DCC Public Safety. This Procedure shall be subject to and superseded by applicable regulations and laws.

### Scope statement

This Procedure applies to all DCC physical facilities and any person accessing DCC facilities.

### 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.

Physical access to DCC creates security risk, especially access to critical areas such as data centers or areas that provide direct access points to DCC's network. This risk can best be mitigated using preventative controls such as smart badges and other forms of identity management.

### Procedure

1. Adds, changes, and deletions of access privileges resulting from new employee onboarding, changes in employee duties, or termination shall be granted in accordance with Human Resources and Public Safety procedures.
2. The data center and other areas deemed highly restricted shall maintain a Visitor Log.
3. All visits to the data center shall be logged, to include: name, firm represented, and the employee authorizing physical access (escort).
4. Visitor Logs shall be retained for at least three (3) months.

## 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](mailto:servicedesk@DCC.edu), or [contact the CIO or CISO](#).

## Definitions

- **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.
- **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.

- **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