CP 6-8d: Cloud and Infrastructure

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

Procedure summary

Dawson Community College (DCC) shall not use Cloud services for controlled sensitive data unless a contractual agreement exists between DCC and the service provider that has been reviewed and approved by DCC's Business Department, and IT Office, thus protecting the security and confidentiality of data for which DCC is custodian.

Scope statement

This Procedure applies to all third party Cloud relationships that DCC enters into, regardless of whether such relationships are through the central IT department or directly by faculty and staff. Impacted personnel are all staff, faculty, and students, as well as vendors, affiliates, and any other external party that could pose data or operational risk to the college.
Cloud relationships include SaaS, IaaS and other Cloud-based product offerings – as well as Cloud storage services such as DropBox. This Procedure shall be subject to and superseded by applicable regulations and laws.

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.

The advent of Cloud computing has created new and largely unsolved challenges for information security. As custodian of DCC's critical data, DCC is legally liable for the protection of that data wherever it is stored. However, when data is stored in a Cloud system outside of DCC's span of control – we cannot see, administer, restore, or protect that data.
The best that DCC can do is to ensure that any Cloud vendor we engage with has the appropriate information security controls (at least equivalent to DCC's) and that we have contractual indemnity and cyber insurance coverage.
This Procedure seeks to ensure that the appropriate due diligence and controls are in place any time we enter into a relationship with a Cloud vendor.

Procedure

Cloud services

DCC staff, faculty, and students who enter into an agreement for a Cloud service shall:

1. Ensure that contracts obligate the vendor to follow DCC security standards (or better).
2. Evaluate the data ownership and ensure the data belongs to DCC or the student.
3. Ensure there is a Non-disclosure Agreement (NDA) in place.

Shared hosting environment

1. All entity or customer data hosted on shared hosting environments shall be managed and protected in accordance with industry best practices.
2. If entities are allowed to run their own applications, these application processes shall run using the unique ID of the entity.
   (For example: no entity on the system may use a shared web server user ID).
3. All CGI scripts used by an entity shall be created and run as the entity's unique user ID.
4. The user ID of application processes shall not be a privileged user (root/admin).
5. Each entity shall have read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, etc.). Also, an entity's files may not be shared by group.
6. Entity's users shall not have write access to shared system binaries.
7. To ensure that each entity cannot monopolize server resources to exploit vulnerabilities (error, race and restart conditions resulting in, for example, buffer overflows), restrictions shall be in place for the use of system resources such as disk
   space, bandwidth, memory and CPU.
8. Logs shall be available for review by the owning entity and the log locations must be clearly communicated to the owning entity.
9. Viewing of log entries shall be restricted to the owning entity.
10. In the event of a compromise, a timely forensics investigation of related servers shall be conducted according to the Incident Response Plan and Procedures.

SERVICE PROVIDER RISK ASSESSMENT

1. There shall be a documented process for engaging service providers that includes proper due diligence prior to engagement.
2. If controlled sensitive data is shared with service providers, then contractually the following shall be required:
   1. Initial risk assessment of the service provider prior to engaging, the level of detail dependent upon the risk of the relationship. This risk assessment may include NDA/confidentiality sign-offs, access controls, and background investigation reviews, as well as review of service provider formal risk assessment reports (Request for "Affiliate" Access to DCC Resources)
   2. An agreement that includes acknowledgement that the service provider is responsible for the security and privacy of DCC confidential (customer) data in the possession of the provider.
   3. Procedures in place for identifying security vulnerabilities.
   4. Management approval for all service provider contracts.
   5. Allowance for monitoring of compliance of security control requirements and identified reporting requirements for possible breaches and non-compliance situations.
   6. Maintain a list of service providers, along with contact information.

7. Implement a monitoring program that assesses the service provider's security posture on at least an annual basis and that provides overall risk assessment of the service provider relationship.

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

- Bandwidth
  The amount of traffic that a computer network can support.
  - Technically, the bit rate of available or consumed information capacity expressed typically in metric multiples of bits
    per second.
  - Variously, bandwidth may be characterized as network bandwidth, data bandwidth, or digital bandwidth. Bandwidth determines the performance of the network. Just as a highway can become gridlocked with too many cars, insufficient bandwidth to support data (especially during peak times like Fall Enrollment) can gridlock the network.
- Buffer
  Part of a computer's operating system designed to temporarily store data in order to increase the efficiency of data processing.
  - A data buffer (or just buffer) is a region of a physical memory storage used to temporarily store data while it is being moved from one place to another. Typically, the data is stored in a buffer as it is retrieved from an input device (such as a microphone) or just before it is sent to an output device (such as speakers).

- Buffers are typically used when there is a difference between the rate at which data is received and the rate at which it can be processed, or in the case that these rates are variable. For example, in a printer spooler or in online video streaming.

- Central Processing Unit (CPU)
  The "brains" of a computer.
  - CPU is the electronic circuitry within a computer that carries out the instructions of a computer program by performing the basic arithmetic, logical, control, and input/output (I/O) operations specified by the instructions.
- 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' Panther Hub is another example of Cloud technology.
- Common Gateway Interface (CGI)
  A standard protocol for web servers to interface with executable programs running on a server that generate web pages dynamically.
- 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.
- Enterprise Computing
  The sum of computer systems, applications, and infrastructure designed to support large, complex organizations or business functions.
  - Usually seen as a collection of big business software solutions to common problems, such as resource management and streamlining processes, running on an enterprise network and using specialized technologies like high performance servers.
  - Today, enterprise computing can be supported using Cloud services such as Software as a Service (SaaS), Infrastructure as a Service (IaaS), etc.
- 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.
- Memory
  The computer hardware component used to store data for immediate use by the CPU (as opposed to data that is persistently stored on the computer hard disk).
- Service Provider
  (In IT) A company that provides its subscribers access to the Internet.
- 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.
- System Binary
  A package of program code that can be understood and executed by a computer's operating system.
- 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."
- Third Party Services
  Any service provided to DCC by an external party or vendor. Today, this is particularly relevant with respect to Cloud based "Software as a Service" (SaaS) providers.
  - Includes, but is not limited to, personal ISPs, free email providers (Gmail, Yahoo, etc.), Cloud-based collaboration and data storage providers (e.g. DropBox), social media sites (e.g. FaceBook, LinkedIn), etc. The security of third party providers cannot be reasonably evaluated and guaranteed by DCC.
- 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