CP 6-8b Backups

COLLEGE PROCEDURE: Backups
CP 6-8b APPROVED: Backups
EFFECTIVE: November 11, 2021
REVISED: November 11, 2021
REFERENCES: N/A

Procedure Summary

All enterprise systems and all confidential and private information shall be backed-up and recoverable in accordance with Dawson Community College (DCC) Business Continuity requirements. This Procedure shall be subject to and superseded by applicable regulations and laws.

Scope statement

This Procedure applies to all system and application backups, whether performed by employees or third parties. Accountable and responsible individuals are the Information Security team and IT operational support personnel. For DCC systems supported and maintained by third parties, such parties are also subject to this Procedure. Others in scope are users of DCC IT Resources as it applies to adhering to best practices for their data storage.

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.

Having secure and accessible data backups is essential for recovery from a disaster or security incident. Malware such as Ransomware can cause data to be inaccessible, other malware can corrupt data or damage storage devices and natural or manmade disasters can result in having to rebuild entire system environments. A strong and articulated backup Procedure supports best practices and mitigates risk of data loss and operational disruption.

To achieve this goal, it is essential that mission critical data be stored in recoverable IT Resources.

Procedure

1. Scheduled backups shall be made of structured data stored in enterprise databases in accordance with defined business recovery need.

2. Unstructured (i.e. personal/file-based data) mission-critical and controlled sensitive data, as well as any other data that is required to be recoverable, shall be stored on shared network drives or Google Drive, and not stored on local drives (e.g.
   C:Drive), portable media or third party platforms.
3. Privacy and security considerations shall be considered before collecting, processing, sharing, or storing institutional or personal data on the cloud.
4. Controlled sensitive data shall not be stored in third party cloud services unless there is a contractual agreement between DCC and the service provider (e.g. DCC's Google contract) that protects the confidentiality and recoverability of the data.
5. Cloud services that store DCC data shall be approved by the Chief Information Security Officer (CISO).
6. Offline storage media used for archival or backup purposes shall be handled and retained in a secured environment in which only DCC personnel and contracted storage facility personnel have access to the archival media.
7. All media couriers and transport mechanisms shall be certified by the CISO.
8. All media transferred from one location to another (or retrieved from archive) shall be logged to a Backup Media Transfer Log to record what is being transferred, by whom, where, and whether it was properly received, and will include signature from management.
9. All media containing controlled sensitive data shall be classified and identified as such prior to transfer.

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

- Backup
  The copying and archiving of computer data so it may be used to restore the original after a data loss event.

- Backups are copies of data taken periodically (usually nightly) and stored offsite for the purpose of archiving, regulatory compliance, and data-loss recovery.

- Chief Information Security Officer (CISO)
  Senior manager responsible for information security compliance at DCC.
- 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.
- 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.
- Malware
  Short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, Trojan horses, and spyware.
- 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 software's 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.

- 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