CP 6-8a: Anti-Malware

COLLEGE PROCEDURE 6-8a: Anti-Malware
APPROVED: Anti-Malware
EFFECTIVE: November 11, 2021
REVISED: November 11, 2021
REFERENCES: N/A

Procedure Summary

All Dawson Community College (DCC) Information Technology (IT) resources potentially vulnerable to viruses or other malware, whether managed by employees or third parties, shall be protected by approved software.
This Procedure shall be subject to and superseded by applicable regulations and laws.

Scope statement

This Procedure applies to all DCC IT resources. 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.
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.

DCC's Defense in Depth strategy seeks to prevent the intrusion and activation of malicious software, commonly referred to as "malware". There are various types of malware and prevention may require different techniques and technologies. This Procedure seeks to protect the college, students, faculty, and staff from the adverse impact of malware infection.

Procedure

1. The Chief Information Security Officer (CISO) shall approve anti-malware software for use on all applicable IT resources.
2. Anti-malware software shall be configured to receive automatic updates, perform periodic scans, and log events.
3. Users shall not configure or disable the anti-malware software.
4. Signatures for anti-malware software shall be automatically updated at least once per day.
5. Systems running DCC anti-malware software shall alert the information security team in real time of the detection of a virus. The CISO will determine what steps to take based on the Risk Management Procedure and best practices.
6. Retention of anti-malware software logs shall be in accordance with the Data Retention and Disposal Procedure (BP 8104).

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.

Definitions

- Anti-Malware Software

  In this use, applies to all software designed to detect and destroy computer viruses, malware, adware, or other malicious software.

- 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.

- 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.

- 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.

- Internet

  A global network that facilitates electronic communication of data between any participating parties.

  - A network of networks that consists of private, public, academic, business, and government networks of local to global scope linked by a broad array of electronic, wireless, and optical networking technologies.

- 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.

- Network

  (In IT) The technology that carries messages between one computer and another.

  - A network is a primary component of technology infrastructure and consists of hardware (e.g. routers, switches) that control and direct traffic; transport technologies (e.g. cables, fiber, wireless radio waves) that transport messages from Point A to Point B; and standards (e.g. Internet Protocol, Ethernet) that facilitate a common understanding of the messages being sent and how they are to be processed.
  - End points (or nodes) on a network are the senders and receivers of the messages and are usually computers (e.g. servers, desktops, laptops) – but can also be technology such as machine controllers, audio/visual devices, etc.
  - The Internet of Things (IoT) largely replaces people interacting across a network with machines and other technology devices interacting across a network, often using artificial intelligence (AI).

- Signature

  (In IT) Digital signatures are proxies for human signatures on electronic documents; malware/virus signatures are unique values that indicate the presence of malicious code used by antivirus software to detect infections.

- 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