COURSE OUTLINE

Section 1:

Course Title: Network and Information Security

Course Code: CNET-1050

Course Description: An examination of information and computer system security. Students investigate security equipment and methods designed to protect a business from security threats. Threat analysis, business continuity, incident response plans, security policies and procedures, cryptography, and securing online transactions are also studied. This course prepares students to obtain the Security+ certification.

Grade Scheme: □ Pass/Fail ☒ Percentage Minimum Pass Mark: 60%

Course Value: Outcome hours OR 3 Credit(s) 60 (30 class + 30 lab) Hours

Pre-requisites: CMPS-1000 A+ Software

Co-requisites: CNET-1021 Cisco CCNA II: Routing and Switching Essentials

Section 2:

Learning Outcomes and Competencies

1. Examine the basic areas of computer security that comprise the first line of defense against security attacks.

1.1 Compare and contrast access control methods.

1.2 Explain the major areas of authentication.

1.3 Describe industry guidelines for strong passwords.

1.4 Explain the various password cracking techniques.

1.5 Reduce the security risks of non-essential services and protocols.

1.6 Describe security risks of default accounts.

1.7 Describe the types of malicious software.

1.8 Use Common Vulnerabilities and Exposure lists to discover known security vulnerabilities.

2. Examine computer network infrastructure and related security issues.

2.1 Describe security concerns of various network devices and applications.

2.2 Explain common types of security attacks.

2.3 Describe the security concerns of media.

2.4 Describe the concepts of security network topologies.

2.5 Compare and contrast the various types of intrusion detection systems.

2.6 Describe the importance of security baselines.

3. Examine how cryptography is used to secure information.

3.1 Compare and contrast encryption algorithms.

3.2 Explain hashing functions and their use in information security.

3.3 Explain the concepts of Public Key Infrastructure.

3.4 Describe the role of Certificate Authorities (CA) in providing mutual authentication.

3.5 Describe digital signatures and their role in providing non-repudiation.

3.6 Explain the importance of key management.

4. Investigate common security technologies.

4.1 Describe the major protocols to secure remote access.

4.2 Describe techniques to secure email.

4.3 Describe protocols to secure Internet communications.

4.4 Describe protocols to secure file transfers.

4.5 Describe major wireless technologies and their security concerns.

4.6 Describe protocols to secure wireless devices.

4.7 Describe tools and techniques to secure mobile devices.

5. Investigate areas of operational and organizational security.

5.1 Explain physical security of equipment and systems.

5.2 Explain user policies and procedures related to security.

5.3 Explain corporate policies and procedures related to security.

5.4 Explain the importance of security education and training for employees.

5.5 Explain access privilege management.

5.6 Describe controls to secure file storage and printing systems.

5.7 Explain how to reduce the security risks due to social engineering.

6. Implement solutions to ensure the security of computer systems and networks.

6.1 Install antivirus/antispyware software according to manufacturer's specifications.

6.2 Configure and maintain antivirus/antispyware solutions to ensure effective protection for client.

6.3 Install a wireless LAN using hardware appropriate to a client's environment.

6.4 Implement security solutions, including encryption, to manage a wireless LAN.

6.5 Configure small office/home office firewall devices to protect a network.

6.6 Configure personal firewall software to protect computer systems.

6.7 Implement operating system hardening practices to secure networked systems.

6.8 Update and patch application software to eliminate vulnerabilities.

7. Perform assessments and audits to ensure adequate security.

7.1 Explain ethical hacking.

7.2 Explain the steps required for risk management.

7.3 Conduct vulnerability assessments.

7.4 Audit security policies and procedures to determine effectiveness.

8. Develop disaster recovery plan to ensure business continuity.

8.1 Explain redundancy planning.

8.2 Describe the key components of a disaster recovery plan.

8.3 Develop procedures for disaster recovery.

8.4 Explain computer forensics.

8.5 Develop incident response procedures.

Section 3:

Assessment Categories:	Projects and Assignments	50%
	Theory tests and exams	40%
	Professionalism	10%

Research Component? □ Yes ☒ No

Section 4:

(For administrative use only)

Is this course new? □ Yes ☒ No

Is this course replacing an existing course(s)? □ Yes ☒ No

If this course is replacing another, please record the name and code of the old course:

Course equivalents: NONE

Note: See Quality Procedure A01 for more details.

Catalog Year of Original Course Implementation: **2011**

Catalog Year of Current Version Implementation: **2015**

Revision level: 3 **Version:** 3 **Date:** June/2016 **Authorized by:** MLGJ

Accreditation and or Supporting Documents:	National Technology Benchmarks: Canadian Council of Technicians & Technologists; Discipline: Information Technology; Level: Technologist
Additional Information:	None
Subject matter expert(s):	Lino Forner

Approved by: (Program Manager)

Paul Murnaghan Date Approved: **2016-06-30**

Approved by: (Curriculum Consultant)

Mary Lou Griffin-Jenkins Date Approved: **2016-06-30**