INFORMATION SYSTEMS SECURITY

Program Outline

Major: INSS
Length: 1 Year
Delivery: 3 Semesters
Credential: Ontario College Graduate Certificate
Effective: 2016-2017
Location: Barrie
Start: Fall (Barrie)

Description
This program prepares students for careers involving the development, evaluation, and support of IT security solutions. Building on previous educational experience, students learn to create cost effective and secure computing environments. Graduates are able to categorize, design, implement, and integrate technical and managerial safeguards to ensure the security of networked computer systems. An emphasis will be placed on interpersonal, organizational, technical, communication, and problem-solving skills applied to enhance the effective implementation of security in a business environment.

Career Opportunities
The need for organizations to build and maintain secure network and information systems has created demand for skilled computer and network systems security specialists. Chief Information Officers and Information Technology Managers charged with the need to plan and implement security controls and infrastructure to protect corporate information systems will increasingly require the skills of security specialists. Career opportunities will be available in both public and private sector organizations. Graduates may gain employment as administrators, technicians or security analysts.

Program Learning Outcomes
The graduate has reliably demonstrated the ability to:

- deploy and manage desktop and server operating systems and optimize system settings in order to 'harden' information systems;
- establish best practices to protect business resources from vulnerabilities and exploits;
- develop security strategies for the deployment of network security procedures and network security devices;
- establish security plans and strategies for proper use and protection of information assets including contingency and disaster plans in compliance with best practices, standards, and regulations;
- create acceptable use policies for business information systems;
- apply project management tools and principles in the building and deployment of security policies and strategies;
- perform security audits using log management software and log analysis to ensure compliance with security plans, policies, standards, and regulations and present results to senior management;
- deliver an effective security awareness and training program to ensure compliance with security policies;
- apply basic entrepreneurial strategies to identify and respond to new opportunities in the information security field;
- investigate and employ environmentally sustainable practices within the information security field.

The Program Progression:

```
Fall Intake - Barrie

Sem 1 | Sem 2  | Sem 3
----------------------
Fall  | Winter | Summer
2016  | 2017   | 2017
```

Admission Requirements:

- Post-secondary diploma or degree with a focus in computer studies, or equivalent work experience in computer networks and operating systems.

Selection Process:

Applicants will be asked to submit a current resume and letter of interest to the Program Coordinator. Academic and experiential learning of all applicants will be assessed.

Criminal Reference/Vulnerable Sector Check:
Placement agencies require an up-to-date clear criminal reference check and vulnerable sector check prior to going out on placement. Students should obtain their criminal reference three months prior to placement; checks conducted earlier may not be considered current. As some jurisdictions require longer lead-time for processing, please check with the program coordinator to ensure you allow for sufficient turn-around time. It is the students responsibility to provide the completed document prior to placement start.

NOTE: A record of criminal offences, for which a pardon has not been granted, may prevent students from completing their placements, thereby affecting their ability to graduate.

Additional Information:
To be successful in this program, you are required to have a personal notebook computer (either PC or Mac architecture) prior to the start of the program that meets or exceeds the following hardware specifications:
- Intel I3 processor or AMD equivalent
- 4GB of memory
- 250GB hard drive

Additional operating systems, security tools, and software used in the program will be provided to the student upon commencement of the program.

Graduation Requirements:
12 Mandatory Courses
1 Internship

Graduation Eligibility:
To graduate from this program, a student must attain a minimum of 60% or a letter grade of P (Pass) or S (Satisfactory) in each course in each semester. The passing weighted average for promotion through each semester and to graduate is 60%.

Mandatory Courses
NETS1006 Contingency Planning and Disaster Recovery
NETS1015 Security Management
NETS1025 Network Security 1
NETS1026 Windows Systems Security

NETS1028 Linux Systems Security
NETS1030 Networks Security 2
NETS1032 Digital Forensics
NETS1034 Hacking Techniques and Exploits
NETS1035 Applied Cryptography
NETS1036 Information Security
NETS1037 Monitoring and Log Management
NETS1038 Application Security

Internship
NETS1033 Computer and Network Systems Security Internship

Course Descriptions:

NETS1006 Contingency Planning and Disaster Recovery 42.0 Hours
This course examines the methods and techniques used to safeguard organizations from serious threats to the normal continuation of business activities due to disastrous events and unplanned disruption to essential services. Students will learn the difference and relationship between Business Recovery Planning and Disaster Recovery Planning, and how to apply the principles of each. Emphasis will be placed upon the practical application of vulnerability and risk assessment, planning, strategies for recovery and implementation of plans and policies.

NETS1015 Security Management 42.0 Hours
This course emphasizes the development and promotion of an information security mission for an organization in accordance with its overall goals and objectives. Students will learn how to identify the roles and responsibilities of each member of an organization in order to develop controls that provide security while maintaining adequate access. Issues such as employment practices, procedures and agreements will be discussed along with policy formation, security awareness training and data classification.

NETS1025 Network Security 1 42.0 Hours
Students learn that controlling network information access is critical to information systems security. Various types and techniques of network access control, rights and permissions are studied, as well as local network and remote access authentication and identification techniques. This course also examines the equipment, methods, and protocols used for the transmission and protection of information. Other topics studied include email and web security, attacks and countermeasures, fraud and abuse.

NETS1026 Windows Systems Security 42.0 Hours
In this course, students learn to apply security industry best practices and to harden the Windows operating system in a variety of configurations and roles. Students learn how

to protect Windows-based systems from attacks, reconfigure the operating system to fully protect it, and scan hosts for known security problems. By the end of the course, students have a solid understanding of the security architectures used by Windows operating systems.

NETS1028 Linux Systems Security 42.0 Hours
In this course, students learn how to secure all major aspects of Linux/Unix operating systems, balancing security issues with the purpose of the system and the needs of an organization. Students learn how to tune kernel and operating system parameters, deactivate components, and tighten the components that remain. By the end of the course, students have a solid understanding of the security architectures used by many Linux and Unix operating systems.

NETS1030 Networks Security 2 42.0 Hours
The Network Security 2 course focuses on the overall security of a network. It expands on the knowledge gained in Network Security 1 and establishes the concepts of intrusion prevention and virtual private networks. Topics include security technologies, products and solutions; firewall and secure router design, installation and configuration; intrusion prevention implementation using routers; and virtual private network implementation using routers and firewalls.
P- NETS1025 Network Security 1

NETS1032 Digital Forensics 42.0 Hours
In this course, students apply the principles of computer forensics in order to detect, track, and analyze digital evidence. Students collect, examine, and interpret data collected from various sources. They learn how to answer key questions about program execution, file opening, network usage, and processes. Students also learn how to use multiple open source forensic tools to track malicious activity that can be used in an investigation.

NETS1033 Computer and Network Systems Security Internship 560.0 Hours
The Internship component of the Computer and Network Systems Security program is a process by which students integrate their academic education with work experience related to their program of study. This integration reinforces skills and theory learned during academic semesters; develops professional contacts, job knowledge and career paths; improves human relations and communications skills, and promotes personal maturity and financial independence.
P- NETS1015 Security Management and P- NETS1026 Windows Systems Security and P- NETS1028 Linux Systems Security and P- NETS1030 Networks Security 2 and P- NETS1032 Digital Forensics and P- NETS1035 Applied Cryptography

NETS1034 Hacking Techniques and Exploits 42.0 Hours
In this course, students examine the current trends in hacking and exploitation. Students learn how to create exploits as a way to prevent, detect, and combat them.

Buffer overflows, race conditions, and unvalidated inputs are examined. This course addresses the latest attack vectors and older attacks that are still prevalent. Evasion of anti-virus and intrusion detection systems are explored. Students walk through many real world attacks used by penetration testers.

NETS1035 Applied Cryptography 42.0 Hours
This course examines cryptography and secure communications. Topics include cryptographic algorithms and protocols, digital signatures, and public key infrastructure. Students will learn how to install and configure encryption technologies for the network, email, and operating system to prevent attacks. Students will examine technologies such as SSH, OpenVPN, IPsec and TrueCrypt. Students will be provided with a comprehensive survey of modern cryptography.

NETS1036 Information Security 42.0 Hours
This course examines the concepts and techniques for designing and implementing large, reliable, secure, and manageable, information security systems. Students learn to analyze business and technical requirements, and select protocols and technologies based on performance and security goals. Students will learn how to install and administer a public key infrastructure, network firewall, intrusion detection system, and network access control system in a cost effective and secure manner.

NETS1037 Monitoring and Log Management 42.0 Hours
In this course, students monitor and analyze system, network, and security events and logs. Students work with enormous amounts of data by managing data retention, filtering, and searching. This course also focuses on how to implement a company-wide log management program and on the daily and weekly tasks of monitoring and alerting.

NETS1038 Application Security 42.0 Hours
Students gain the knowledge and skills to defend against multiple types of application attacks. The Open Web Application Security Project (OWASP) Top Ten is introduced to increase understanding of some of the most popular vulnerabilities and how to defend against them. Students learn how to test applications for vulnerabilities and misconfigurations. Manual and automated tools are used to map, discover, exploit, and secure web applications on the client and server side.

Course Description Legend
P = Prerequisite; C = Concurrent prerequisite; CO= Corequisite

Information contained in College documents respecting programs is correct at the time of publication. Academic content of programs and courses is revised on an ongoing basis to ensure relevance to changing educational objectives and employment market needs. The college reserves the right to add or delete programs, options, courses,

timetables or campus locations subject to sufficient enrolment, and the availability of courses.