Cyber Security Certificate

This Cyber Security Certificate is designed to meet the needs of the present and future Networking, Internet and Cyber Security Professions. This Certificate also is part of the Networking A.A.S. Degree Third Year Advanced Studies Program.

Based on a 2015 Tech Republic IT article:

a. The top 10 Tech Skills to have includes Network and Cyber Security
b. DCC's Cybercrime Investigation, Networking Degree, and Career Studies Certificates meet the majority of the Tech Skills desired by industry today.
c. The top 10 list of IT Certifications include Networking and Cyber Security
d. Salaries that can be obtained for IT Networking and Cyber Crime and Security Professionals range from $56,277 to $85,699
e. With the addition of industry certification, educational background, and work experience these salaries have shown to go even higher.

Purpose: This Cyber Security Certificate curriculum is designed for those individuals who are presently in the field of IT or related IT Security field who desire to expand their knowledge and capabilities to meet the needs of current and future IT Professions. This certificate and the courses it contains are mapped to the NSA/DHS (**National Security Agency / Department of Homeland Security**) Knowledge Units necessary for Danville Community College.

Credit for Prior Learning: Students in this program may be eligible to receive credit for prior learning. See an academic advisor or counselor for further information.

Transfer Information: Danville Community College has articulation agreements with selected senior institutions. Students interested in transfer opportunities should contact their academic advisor early in the program for specific course requirements.

Required Background: Due to the level of knowledge required in Information Technology, candidates must meet one (1) or more of the following criteria:

A. Professional background in IT Networking. Individual may be required to demonstrate required skills.
B. Industry Certifications in the field of Networking and/or Security. Candidates will be required to provide evidence of successful completion of each Certification being considered.
C. Completion of courses in Cisco CCNA Networking and Microsoft Server Operating Systems

Cybersecurity Certificate Course Requirements:

First Semester

Course:	**Description**	**Credits Awarded**
ADJ-161	Introduction to Computer Crime	3
ITE-221	Introduction to Client Operating Systems	3
ITN-260	Networking Security Basics	3
SDV-100	College Success Skills	1
==		
TOTALS		**10**

Second Semester

Course:	**Description**	**Credits Awarded**
HUM Elec	General Education Elective	3
ITN-261	Network Attacks, Computer Crime, and Hacking	3
ITN-262	Network Communication, Security, Authentication	4
TOTALS		**10**

Third Semester

Course:	**Description**	**Credits Awarded**
ENG-111	College Composition I	3
ITN-263	Internet/Intranet Firewalls and E-Com Security	3
ITN-276	Computer Forensics I	4
TOTALS		**10**

Fourth Semester

Course:	**Description**	**Credits Awarded**
ITN-254	Virtual Infrastructure/Installation and Configuration	4
ITN-267	Cyberlaw	3
ITN-277	Computer Forensics II	3
TOTALS		**10**

Total Minimum Credits: 40

Catalog Descriptions for Courses:

ADJ 161 Introduction to Computer Crime (3 cr.)
Provides a basic introduction to the nature of computer crime, computer criminals, relevant law, investigative techniques and emerging trends. Lecture 3 hours per week.

ITE 221 PC Hardware and OS Architecture (3 cr.)
Covers instruction about processors, internal functions, peripheral devices, computer organization, memory management, architecture, instruction format, and basic OS architecture. Lecture 3 hours per week.

ITN 260 Network Security Basics (3-4 cr.)
Provides instruction in the basics of network security in depth. Includes security objectives, security architecture, security models and security layers; risk management, network security policy, and security training. Includes the give security keys, confidentiality integrity, availability, accountability and auditability. Lecture 4 hours per week.

ITN 261 - Network Attacks, Computer Crime and Hacking
Encompasses in-depth exploration of various methods for attacking and defending a network. Explores network security concepts from the viewpoint hackers and their attack methodologies. Includes topics about hackers, attacks, Intrusion Detection Systems (IDS) malicious code, computer crime and industrial espionage. Lecture 4 hours per week.

ITN 262 Network Communication, Security and Authentication (4 cr.)
Covers an in-depth exploration of various communication protocols with a concentration on TCP/IP. Explores communication protocols from the point of view of the hacker in order to highlight protocol weaknesses. Includes Internet architecture, routing, addressing, topology, fragmentation and protocol

analysis, and the use of various utilities to explore TCP/IP. Prerequisite: Cisco CCNA Certification or completion of ITN 157. Lecture 4 hours per week.

ITN 263 - Internet/Intranet Firewalls and E-Commerce Security (3 cr.)
Gives an in-depth exploration of firewall, Web security, and e-commerce security. Explores firewall concepts, types, topology and the firewall's relationship to the TCP/IP protocol. Includes client/server architecture, the Web server, HTML and HTTP in relation to Web Security, and digital certification, D.509, and public key infrastructure (PKI). Lecture 4 hours per week.

ITN 254 Virtual Infrastructure: Installation and Configuration (4 cr.)
Explores concepts and capabilities of virtual architecture with a focus on the installation, configuration, and management of a virtual infrastructure, ESX Server, and Virtual Center. Covers fundamentals of virtual network design and implementation, fundamentals of storage area networks, virtual switching, virtual system management, and engineering for high availability. Prerequisite: Approved IT Qualifications or ITN 103. Lecture 4 hours per week.

ITN 267 - Legal Topics in Network Security (3 cr.)
Conveys an in-depth exploration of the civil and common law issues that apply to network security. Explores statutes, jurisdictional, and constitutional issues related to computer crimes and privacy. Includes rules of evidence, seizure and evidence handling, court presentation and computer privacy in the digital age. Lecture 4 hours per week.

ITN 276 Computer Forensics I (4 cr.)
Teaches computer forensic investigation techniques for collecting computer-related evidence at the physical layer from a variety of digital media (hard drives, compact flash and PDAs) and performing analysis at the file system layer. Prerequisite: ITN 106, ITN 107. Co-requisite: ITN 260. Credit will be given to ITN 275 or ITN 276 and ITN 277, but not all three courses. Lecture 3-4 hours per week.

ITN 277 Computer Forensics II (3 cr.)
Develops skills in the forensic extraction of computer evidence at a logical level using a variety of operating systems and applications (i.e., e-mail) and learn techniques for recovering data from virtual memory, temporary Internet files, and intentionally hidden files. Prerequisite: ITN 276, Computer Forensics I. Credit will be given to ITN 275 or ITN 276 and ITN 277, but not all three courses. Lecture 3-4 hours per week.