Moraine Valley Community College

Palos Hills, IL
NSF Regional Center for Systems Security and Information Assurance

IT DATA ASSURANCE & SECURITY SPECIALIST
A.A.S. Degree 62 Credits

General Education Requirements Total 18 Credits

Rhetoric/Speech	6 Credits	
COM-101	Composition I	3
COM-103	Speech Fundamentals	3
Social/Behavioral Sciences	3 Credits	
Select 6 credits from the following:		
ANT, ECO, GEO, HIS, PSC, PSY, SOC, SSC		3
Science and Math	6 Credits	
Select 6 credits from the following:		
BIO, CHM, EAS, GEL, MTH, NAT, PHY, PHS		6
Humanities/Language	3 Credits	
Select 3 credits from the following:		3
ART, FRE, GER, HUM, JPN, LIT, MUS,		
PHI, SPA, THE		
Core IT Technology	20 Credits	
LAN-101	Orientation to IT Professions	1
LAN-103	IT Security Awareness	1
LAN-111	IT Hardware Essentials	3
LAN-112	IT Operating Systems Essentials	3
LAN-121	Managing LAN Hardware	3
LAN-122	Managing Network OS	3
LAN-146	Internetwork Connectivity	3
LAN-246	Introduction to Routing	3
Internet Security Specialty Track	24 Credits	
LAN-153	IT and Data Assurance I	3
LAN-163	IT and Data Assurance II	3
LAN-223	Managing Messaging Services	3
LAN-226	Managing Web Servers	3
LAN-233	Managing Database Services	3
LAN-253	Managing Network Security I	3
LAN-263	Managing Network Security II	3
LAN-273	Network Security Design	3

Moraine Valley Community College
AAS Degree
IT DATA ASSURANCE & SECURITY SPECIALIST

Program Sequence			
Semester One		Semester Two	
COM-101	3	COM-103	3
LAN-101	1		
LAN-103	1	LAN-146	3
LAN-111	3	LAN-246	3
LAN-112	3	LAN-153	3
LAN-121	3	LAN-163	3
LAN-122	3		
Total	17	Total	15
Semester Three		Semester Four	
ART, FRE, GER, HUM, JPN, LIT, MUS, SPA, THE	3	ECO, GEO, ANT, HIS, PSC, PSY, SOC, SSC	3
LAN-253	3	BIO, CHM, EAS, GEL, NAT, PHY, PHS	3
LAN-263	3	LAN-233	3
LAN-226	3	LAN-223	3
MTH	3	LAN-273	3
TOTAL	15	TOTAL	15

NSF Regional Center for Systems Security and Information Assurance (CSSIA)

http://www.cssia.org

CSSIA is developing a comprehensive curriculum in IT security that can be used as a model for many schools. Supporting materials under adaptation and development include: MS PowerPoint slides, tests, lab manuals, lab equipment suggestions, and textbook recommendations. The model includes the following courses:

Security Awareness - This class will discuss security awareness and will walk users through every aspect of Information Security in a very broad, easy to understand way and explain to them the value of securing data, both for themselves and the organization. The class will distribute legislation, local, state and federal privacy policies, and liability of individuals and institutions related to data confidentiality and integrity. The course will introduce risk management, security policies, and common threats and countermeasures. The course will also present best practices in access control and password policies.

Information "Data" Assurance I - The student will be introduced to computer network vulnerabilities and threats and how to safeguard computer networks from those vulnerabilities and threats. This course will expose the student to network security planning, network security technology, network security organization and the legal and ethical issues associated with network security. In this class, students will learn the skills necessary for Security + certification.

Network Security I - This course introduces the network security specialist to the various methodologies for defending a network. The student will be introduced to the concepts, principles, types and topologies of firewalls including: packet filtering, proxy firewalls, application gateways, circuit gateways and stateful inspection. Students taking this class will be prepared to take the SECUR (Securing Cisco IOS Networks) and CSPFA (Cisco Secure PIX Firewall Advanced) exams in preparation for the Cisco Firewall Specialist. These exams also count toward the security professional level CCSP certification. (CCSP - Cisco Certified Security Professional)

Information "Data" Assurance II - This course will go into more depth using the tools and concepts students were exposed to in Information "Data" Assurance I. The student will be introduced to the concepts, principles and techniques, supplemented by hands-on exercises, for defending from an attack. These methodologies are presented within the context of properly securing the network. The course will emphasize network attack defense methodologies with the emphasis on student use of network attack techniques and tools. The concept of Systems Security Certified Practitioner (SSCP) will be strongly emphasized in this course along with several of the CISSP CBK domains (Certified Information Systems Security Professional - Common Body of Knowledge).

Network Security II - This course will expose the student to the various defense methodologies associated with Virtual Private Networks (VPN), Host Intrusion Detection

Systems (HIDS) and Network Intrusion detection Systems (NIDS) will be discussed along with in depth coverage of incident handling and response. It will introduce the student to the best practices associated with properly securing business critical network systems using VPNs.

Network Security Design - This is our capstone course incorporating all of the topics and concepts from the previous classes. Students will be given case studies where they will have to design a total IT security system for a company within a particular industry - Health or Banking, for example. This course will give the network security specialist the opportunity to conduct a vulnerability analysis upon a network in order to practice or refine the attack methodologies with the hacker tools and techniques which the student was exposed to in the previous courses. The student must demonstrate the ability to design, plan and execute a vulnerability analysis against an organization network. The student must prepare a written report of the security design, attack methodology, tools and techniques used.

Computer Forensics I - This course deals with the preservation, identification, extraction, documentation and interpretation of computer data. Topics covered include evidence handling, chain of custody, collection, preservation, identification and recovery of computer data. This course will feature the use of NTI forensics tools.

Computer Forensics II - This course is a continuation of Computer Forensics I, and includes forensic analysis of Linux file systems and introduces additional various forensic analysis software suites used to perform forensic analysis of FAT 16, FAT 32 and NTFS file systems. This course will feature the use of Encase and FTK forensics tools.

Additional Courses - Additional courses are being evaluated and are under consideration for standardization and adoption. Courses currently under evaluation include High-Tech Crime and Cyber Defense exercises. CSSIA will also look to provide faculty development for specialty technologies that are integral components of several courses. Currently the Fundamentals of Wireless Networks course will be offered. The CSSIA Visual Flow provides where these current and future courses relate to our curriculum model. http://cssia.org/CUR_visual.cfm