ASSOCIATE DEGREE COMPUTER INFORMATION SYSTEMS

Whatcom Community College

May 2021

Whatcom
COMMUNITY COLLEGE

Contents

Program Overview

Whatcom's students can choose from two lower division degree paths. The associate of science (AS) degree in computer information systems (CIS) prepares students for careers in the fields of technical support, networking, or information security. The associate of applied science transfer (AAS-T) degree in cybersecurity prepares students to enter the workforce in a variety of high-demand security-related fields. Both options also prepare students to apply to continue in Whatcom's bachelor of apply science (BAS) degree in IT networking - cybersecurity; the AAS-T degree in cybersecurity offers students the additional option to apply to transfer to four-year degree programs at certain colleges and universities.

CIS certificate options in network administration and technical support allow students to acquire employable credentials while working toward degree completion. An information security professional certificate of proficiency is also available. All of these certificates are fully embedded in the AS degree in CIS and partially in the AAS-T degree in cybersecurity.

Program Outcomes- Computer information systems

Upon successful completion of the computer information systems (CIS) degree, CIS - network administration certificate, or CIS - technical support certificate, graduates should be able to...

1. Describe the basics of computer operating systems platforms.
2. Perform the basics of computer and network security.
3. Diagnose and repair personal computers.
4. Communicate professionally with customers and co-workers.
5. Describe and troubleshoot at each layer of the OSI and TCP/IP network models.
6. Design an IP subnetting scheme.

Upon successful completion of the CIS degree or CIS - networking certificate, graduates should *also* be able to...

7. Implement and troubleshoot a variety of network topologies and protocols.
8. Set up and maintain medium-size routed and switched networks.

Upon successful completion of the CIS degree, graduates should *also* be able to...

9. Install, configure and use the tools and techniques of computer forensics.
10. Identify threats and implement countermeasures to ensure network system security.

Degree Requirements

Associate in Science (AS) - Computer Information Systems

The computer information systems degree prepares students for employment in a variety of fields, including technical support/help desk positions, network administration, network technician, and information security specialist. Students with prior experience are encouraged to meet with the program coordinator for placement in the program.

Course requirements (effective fall 2020)

CORE REQUIREMENTS (courses are listed alphabetically)		**Credits**
CIS 104	Unmanned aircraft systems (UAS) piloting	3
CIS 105	Computer operating systems I	5
CIS 106	Open source operating systems	5
CIS 110	Introduction to computer security	3
CIS 116	Virtualization	3
CIS 205	Computer operating systems II	5
CIS 206	Computer support I	5
CIS 214	Network security I	5
CIS 215	Network security II	5
CIS 216	Industrial control systems security	5
CIS 225	Computer forensics	5
CIS 236	Cisco networking I	5
CIS 237	Cisco networking II	6
CIS 238	Cisco networking III	6
Subtotal		**66**
GENERAL EDUCATION REQUIREMENTS/RELATED INSTRUCTION		**Credits**
BUS 170	Customer service for professionals (HR)	3
or CMST OC	Any CMST or CMST& course designated "OC"	5

ENGL& 101	English composition I (CM)	5
Any course designated as computation on the Related Instruction list (CP)		5
Subtotal		**13-15**
ELECTIVES/COOPERATIVE WORK EXPERIENCE		**Credits**
CIS 190	Technical internship	5
Any college level course numbered 100 or above. Recommended disciplines: ACCT, BTEC, BUS, CIS, CJ, CS, ECON, FIN, HTBM, MATH, OFFAD, VISCM; or PSYCH 106.		4 to 6
and/or CO-OP 180	Preparing for career work experience	1 to 2
and/or PSYCH 105	Career search process	3
Subtotal		**9-11**
Total		**90**

Course Descriptions

CIS 104 – Unmanned aircraft systems (UAS) piloting

Credits: 3 (2 lecture, 1 lab)

Course description
This course will teach students about how to pilot an Unmanned Aircraft System (UAS) and proper safety guidelines. Students will learn applicable regulations relating to small UAS rating privileges, limitations, flight operation and more.

Course outcomes: Upon successful completion of this course, each student should be able to...
1. Explain FAA safety guidelines for UAS'.
2. Perform proper preflight procedures.
3. Operate a UAS.
4. Explain basic aeronautical concepts.
5. Describe components of a UAS.
6. Maintain components of a UAS.

CIS 105 – Computer operating systems I

Credits: 5 (3 lecture, 2 lab)

Course description
This course introduces the fundamentals of computer operating systems, including history, evolution, and design, as well as support, maintenance, and troubleshooting. Lab work included.

Course outcomes: Upon successful completion of this course, each student should be able to...
1. Describe the boot process and the basic interactions between hardware and software.
2. Install and update an operating system.
3. Perform the daily tasks involved in managing and troubleshooting operating systems.
4. Use the command line to perform routine tasks.
5. Identify and interpret system events logged on a system.
6. Describe and demonstrate file security and file sharing methods.
7. Backup, modify, and recover critical files.
8. Carry out the recovery of a failed system.

CIS 106 – Open source operating systems

Credits: 5 (3 lecture, 2 lab)

Course description
This course examines the fundamental management of open source systems from the command line, user administration, file permissions, software configuration, and management of clients.

Course outcomes: Upon successful completion of this course, each student should be able to...
1. Use scripting languages to write simple scripts to automate system administration tasks.
2. Use Linux command interpreters.
3. Use the Linux file system and its basic operations.
4. Apply secure practices.
5. Create, modify, and remove user and group accounts.
6. Monitor and modify running processes.
7. Implement and maintain various open source server applications.

CIS 110 – Introduction to computer security

Credits: 3 (2 lecture, 1 lab)

Course description
This course examines the basics of computer security, including identifying threats, planning for business continuity, and preparing for various security attacks.

Course outcomes: Upon successful completion of this course, each student should be able to...
1. Explain and differentiate the security principles of confidentiality, integrity, and availability.
2. Distinguish types of malware and attacks.
3. Apply tools and techniques for vulnerability assessment.
4. Implement host security.
5. Explain the security function and purpose of network devices and technologies.
6. Identify types of authentication and perform basic configuration.
7. Distinguish types of cryptography and their uses.
8. Implement basic mobile security.

CIS 116 – Virtualization

Credits: 3 (2 lecture, 1 lab)

Course description
Implementing virtualization techniques and technologies.

Course outcomes: Upon successful completion of this course, each student should be able to...
1. Set up and configure a virtual network.
2. Troubleshoot virtual network issues.
3. Secure virtual networks.
4. Apply virtualization to the workplace.
5. Implement disaster recovery.

CIS 205 – Computer operating systems II

Credits: 5 (3 lecture, 2 lab)

Course description
Advanced study of computer operating systems and platforms.

Course outcomes: Upon successful completion of this course, each student should be able to...
1. Manage a Windows Server environment.
2. Administer configuration of Active Directory and related services.
3. Summarize Active Directory design and account management methods.
4. Implement Group Policy configuration and management.
5. Employ Active Directory Certificate Services.
6. Perform implementation of Internet Information Services for Web Services.

7. Implement installation of Virtualized networks using Hyper-V.
8. Conduct command line configuration and management using Core Server and PowerShell.

CIS 206 – Computer support I

Credits: 5 (3 lecture, 2 lab)

Course description
In-depth study of computer components and their interrelationships. Lab period with hands-on experience in installation, upgrading, removal, configuration, and troubleshooting of software and hardware.

Course outcomes: Upon successful completion of this course, each student should be able to...
1. Identify all parts of a basic personal computer.
2. Discuss the functions and interactions of PC subsystems.
3. Select quality PCs and constituent components based on performance and cost.
4. Perform installation, replacement, and upgrades of PC hardware components and peripherals.
5. Implement and troubleshoot a simple Local Area Network.
6. Troubleshooting and repair faulty PC components and peripherals.
7. Generate Help Desk reports.
8. Use customer support skills and techniques.

CIS 214 – Network security I

Credits: 5 (3 lecture, 2 lab)

Course description
This course examines network security fundamentals, including defining a security policy, attack methods, intrusion detection, firewalls, identifying risks, and securing networks.

Course outcomes: Upon successful completion of this course, each student should be able to...
1. Describe and implement authentication measures.
2. Create a secure networking environment.
3. Describe and demonstrate attacker methodology.
4. Identify different security topologies.
5. Describe firewalls and physical security concepts.
6. Demonstrate the daily tasks involved with managing and troubleshooting security technologies.
7. Create a security policy.

CIS 215 – Network security II

Credits: 5 (3 lecture, 2 lab)

Course description
This course is a continuation of Network Security I, with added emphasis on defense in depth.

Course outcomes: Upon successful completion of this course, each student should be able to...
1. Implement an incident response plan.
2. Apply defense in depth techniques.
3. Design a secure network topology.
4. Securely configure hosts and servers.
5. Implement network perimeter defenses.
6. Implement remote access.

CIS 216 – Industrial control systems security

Credits: 5 (3 lecture, 2 lab)

Course description
Securing Industrial Control Systems including identifying risks, configuring devices and protocols, attack methods, and security ICS networks.

Course outcomes: Upon successful completion of this course, each student should be able to...
1. Describe Supervisory Control and Data Acquisition (SCADA) and control systems.
2. Configure devices.
3. Describe ICS Protocols.
4. Describe risks to Industrial Control Systems.
5. Demonstrate exploits and attack methods against Industrial Control system devices.
6. Implement Intrusion Detection.
7. Implement Industrial control systems network security, identification and remediation.

CIS 225 – Computer forensics

Credits: 5 (3 lecture, 2 lab)

Course description
This is an introductory course to computer forensics and investigations. Topics include: forensic tools, computer forensic analysis, investigations, and preparing written reports.

Course outcomes: Upon successful completion of this course, each student should be able to...
1. Acquire and preserve evidence from non-volatile storage media.
2. Acquire and preserve live evidence from a running system.

3. Use forensics tools through all phases of an investigation.
4. Analyze forensic evidence in file systems.
5. Analyze forensic evidence in operating system structures within file systems or live captures.
6. Analyze forensic evidence in memory.
7. Analyze network captures and logs.
8. Document and present the results of a forensics investigation.

CIS 236 – Cisco networking I

Credits: 5 (3 lecture, 2 lab)

Course description
First in the three quarter networking sequence. This course introduces the fundamentals of networking, including introduction to the OSI and TCP/IP network models, and IP addressing and sub-netting. Other topics include: network design, topologies, protocols, wiring, network devices, and network security fundamentals.

Course outcomes: Upon successful completion of this course, each student should be able to...
1. Explain the layers of communications in data networks using network protocol models.
2. Configure and verify network device interfaces.
3. Configure subnet masks and addresses.
4. Build a simple Ethernet network using routers and switches.
5. Employ basic cabling and network designs to connect devices.
6. Perform basic router and switch configuration and verification using Cisco CLI commands.

CIS 237 – Cisco networking II

Credits: 6 (3 lecture, 3 lab)

Course description
Topics include: LAN Switching, Routing and wireless communication, configuring, verifying, troubleshooting VLANs, inter-VLAN routing, DHCP, routing and switching redundancy, STP, and trunking on Cisco devices. Students will learn to configure wireless networks and common implementation issues. Students will gain hands on experience in the lab.

Course outcomes: Upon successful completion of this course, each student should be able to...
1. Configure, verify, and troubleshoot VLANs, interVLAN routing, VTP, trunking on Cisco switches, and STP operation.
2. Perform comprehensive routing configuration skills.
3. Design and implement a redundant routing and switching environment.
4. Perform basic router and switch configuration and verification using Cisco CLI commands.

5. Apply basic network security configurations to a network.

CIS 238 – Cisco networking III

Credits: 6 (3 lecture, 3 lab)

Course description
Topics include: WAN technologies, Quality of Service, Network security, Network management and automation. WAN security concepts are discussed in detail, including types of threats, how to analyze network vulnerabilities, and general methods for mitigating common security threats.

Course outcomes: Upon successful completion of this course, each student should be able to...
1. Troubleshoot common network problems using a layered model approach.
2. Design and interpret network diagrams.
3. Perform and verify initial network device configuration tasks including remote access management.
4. Configure, verify, and troubleshoot LAN and WAN technologies.
5. Manage IOS configuration files.
6. Identify the basic parameters to configure a network and common implementation issues.

CIS 190 – Technical internship

Credits: 5 work site (165 hours)

Course description
Students develop practical skills by applying what is learned in the classroom with planned, supervised, on the job experience. Students explore technical and career issues related to the profession, including ethic, responsibility, critical thinking, and problem solving skills. Repeatable for credit with program permission.

Course outcomes: Upon successful completion of this course, each student should be able to...
1. Create a personalized site specific plan of learning to execute while at the work site.
2. Integrate classroom theory with practical, work site experience.
3. Demonstrate professional behavior in all interactions and communications.
4. Assess their own technical knowledge, skills and behaviors (including soliciting feedback from others) to improve their professional practice.