Cybersecurity – AAS

Spring 2019 Outcomes

Old name: Network Administration & Security - AAS

*Fall 2019 change*

1. Use mechanisms available in an operating system to control access to resources.
2. Configure infrastructure server roles.
3. Investigate various countermeasures and security controls to minimize risk and exposure.
4. Support the ethical responsibility of ensuring software correctness, reliability, and safety.
5. Illustrate through examples the concepts of risk, threats, vulnerabilities, attack vectors, and exploits, noting there is no such thing as a perfect security.
6. Analyze known security incidents to trace and document the steps in the incident.
7. Develop Technical Artifacts.
8. Examine ethical issues related to cybersecurity.
9. Write a company wide security policy.
10. Communicate effectively and efficiently with clients, users and peers.
11. Design and build virtual computing environments.
12. Construct input validation and data sanitization in applications, considering adversarial control of the input channel.

**Course Outcomes**

CSCI1110 – Informatics

1. Analyze and evaluate various data transmission methods.
2. Analyze various Information Technology solutions for applicability in various environments.
3. Evaluate data security systems in relation to current legal and social implications.
4. Differentiate between authenticity and authority of different information sources.
5. Identify and select factual information to provide a potential solution to a problem.
6. Interpret and present data conclusions in an appropriate and logical manner for the audience.
7. Organize a small group to evaluate various solutions presented from the data.
8. Evaluate and understand data security methods in relation to legal and ethical requirements in selected regions of the world.
9. Articulate the impact of Information Technology on personal ethics.
10. Evaluate the impact of Information Technology on a chosen field of study.

CPTR1122 - Microcomputer Maintenance

1. Analyze the operation of a microcomputer.
2. Recognize microcomputer system architecture.
3. Examine the various types of computer hardware.
4. Demonstrate hardware troubleshooting skills.
5. Plan the building of a working computer.
6. Analyze the operation of system software.
7. Plan a working operating system installation.
8. Manage a working operating system.
9. Demonstrate operating system troubleshooting skills.
10. Examine the various types of networks.
11. Examine the various types of printers.
12. Examine the various types of portable microcomputers.

ENGL1101 - College Writing

1. Demonstrate the writing process through invention, organization, drafting, revision, editing and presentation.
2. Participate effectively in groups with emphasis on listening, critical and reflective thinking and responding.
3. Locate and evaluate information from diverse academic sources.
4. Synthesize information from diverse academic sources.
5. Construct logical and coherent arguments.
6. Use authority, point-of-view and individual voice and style in writing.
7. Respond critically via discussion.
8. Respond critically via writing.
9. Employ syntax and usage appropriate to academic disciplines and the professional world.
10. Select appropriate communication choices for specific audiences.
11. Use a discipline-appropriate style guide to responsibly credit and document information.

CPTR1106 - Microcomputer Databases

1. Create database reports.
2. Create table relationships.
3. Define referential integrity.
4. Create database queries.
5. Manipulate database data.
6. Perform data import operations.
7. Create data entry forms.
8. Demonstrate database programming concepts.
9. Create database tables.
10. Create and manage a switchboard.
11. Create database macros.

COMM1120 - Introduction to Public Speaking

1. Demonstrate the writing and speaking process through invention, organization, drafting, revision, editing, and presentation.
2. Select appropriate communication choices for specific audiences.
3. Complete speaking evaluations with an emphasis on listening and responding ethically.
4. Demonstrate the ability to make sound rhetorical choices.
5. Write and deliver speeches that demonstrate a clear, critical perspective on speech topic.
6. Demonstrate the appropriate use of verbal and nonverbal delivery.
7. Complete group work with emphasis on cooperative learning and critical thinking.
8. Incorporate diverse and ethical supporting material in the speech-making process.
9. Evaluate the effectiveness of logical and coherent arguments for the purpose of persuasion.

CPTR2272 - Network Operating Systems

1. Manage network accounts and groups.
2. Configure remote network access.
3. Manage network services.
4. Design network domain structures.
5. Describe multi-domain network structures.
6. Create fault-tolerant resource plans.
7. Manage security settings and policies.
8. Analyze network resource utilization.
9. Document network configuration.

3 Credit Elective

* CPTR1170 - Web Engineering I
* CPTR1178 – Robotics
* CSCI1121 - Computer Science I
* CSEC2212 - Web Security

6 credits MnTC

CPTR1108 - CISCO 1

1. Compare various networking models.
2. Compare the various types of networking media.
3. Demonstrate a working knowledge of the TCP/IP protocol stack.
4. Recognize the components involved with assembling a network.
5. Design and assemble small working networks.
6. Recognize the tools necessary to troubleshoot networks.
7. Solve network hardware and software problems.
8. Use network monitoring tools to troubleshooting equipment failures.
9. Explain IP addressing and subnetting.

CPTR1001 - Introduction To Programming and Scripting

1. Describe the features and syntax of a programming language.
2. Understand how software can be written to solve business problems.
3. Use debugging and testing to create error-free code.
4. Demonstrate industry standard code development techniques.
5. Develop logic structures.
6. Develop loop structures.
7. Develop control structures.
8. Understand datatypes.
9. Understand functions.
10. Create, update, and process data files.
11. Understand techniques required for security in computer programming.

CSEC2204 - Managing Directory Services

1. Describe the structure of Active Directory.
2. Describe the philosophy of directory services.
3. Explain the role of Domain Name Services in Active Directory.
4. Design an Active Directory architecture.
5. Install Domain Name Services using current best practices.
6. Implement Active Directory replication to current standards.
7. Create an Active Directory auditing plan.
8. Employ current authentication and authentication methods.
9. Demonstrate proper management of objects.
10. Monitor Active Directory performance.
11. Demonstrate proper planning for disaster recovery.
12. Apply software management using group policy.
13. Implement group policy on Active Directory objects.
14. Employ Active Directory operation masters.
15. Troubleshoot Active Directory

HUM2236 - Technology in the Humanities

1. Students will demonstrate an understanding of the relationship between advances in technologies and changes in the daily lives of societies that adopt them.
2. Students will be able to recognize how various technologies have impacted on today's social order and anticipate advantages and difficulties associated with emerging technologies
3. Students will be able to draw connections between advances in technology and inevitabilities such as changes in how education is demanded and delivered
4. Students will be able to identify specific philosophical, political and social movements and how they helped foster technical innovation or prevent natural technical evolution
5. Students will recognize how changes in technology such as paint, sound recordings and motion pictures have affected the range of expressions available to artists.
6. Students will demonstrate the importance of understanding technology both an aid to ethical and productive self expression and a hindrance to responsible social interaction.
7. Students will draw connections between modes of expression and associated limitations resulting from inequities in education and economic and social class.
8. Students will demonstrate an understanding of how major technical advances such as the printing press promoted global communication and cultural exchanges.
9. Students will be able to identify which applications of modern technology improve ethnic diversity and which applications promote intolerance.
10. Students will be able to identify which apparently small improvements in military technology were responsible for major political changes on a global scale.
11. Students will be able to posit workable solutions for addressing inequities in matters of global social and economic development imposed by changes in technology.

CPTR1118 - CISCO 2

1. Maintain router operating system.
2. Analyze a router boot process.
3. Examine components in a router.
4. Use router command line editing.
5. Identify layer three routing protocols.
6. Configure routing protocols.
7. Configure a router to connect to a network.
8. Develop an access list.
9. Configure access lists.
10. Troubleshoot router connectivity.
11. Troubleshoot a routed network.

CPTR2224 - Linux I

1. Create Linux accounts.
2. Manage Linux accounts.
3. Prepare appropriate documentation.
4. Analyze graphical environments.
5. Write simple shell scripts.
6. Manage application software.
7. Manage security.
8. Evaluate fault-tolerance solutions.
9. Use appropriate software and commands.
10. Manage printing.

CPTR2236 - Network Security

1. Identify network security threats.
2. Administer encryption and authentication for wireless networks.
3. Examine protecting advanced communications.
4. Identify Web related threats.
5. Perform network hardening.
6. Examine e-mail threats.
7. Configure VPNs for secure sessions.
8. Analyze remote access security and social engineering threats.
9. Identify software exploits.
10. Examine major types of attacks on information systems.
11. Identify the factors in a secure network strategy.
12. Practice securing web communications utilizing SSL/TLS.
13. Examine cryptography.
14. Apply IPSec policies.
15. Explore the basic computer forensics methods.
16. Plan a patch management strategy for network servers.
17. Analyze the role of firewalls, routers and switches in security.
18. Examine intrusion detection systems.

3 Credits Elective

* CPTR2200 - CISCO 3
* CPTR2208 - CISCO 4
* CPTR2230 - Structured Query Language
* CPTR2234 - Linux II
* CPTR2250 - IT Supervised Occupational Experience
* CPTR2260 - Advanced Structured Query Language
* CPTR2294 – Internship
* CPTR2296 - Topics in Computers
* CSCI1122 - Computer Science II

CPTR2245 - Enterprise Network Technologies

1. Analyze the cause and cost of network downtime.
2. Develop strategies for high availability.
3. Analyze SAN technology.
4. Analyze server virtualization.
5. Analyze active and passive server clustering.
6. Evaluate concepts for cloud computing.
7. Design an enterprise network.
8. Implement server virtualization.
9. Develop electronic documents supporting an enterprise network design.
10. Evaluate options for green technologies.

CSEC2228 - Network Defense

1. Outline physical security measures to current best practices.
2. Identify personnel security practices and procedures.
3. Explain software security best practices.
4. Outline network security.
5. Describe administrative security procedural controls.
6. Define cryptosecurity.
7. Indicate proper key management procedures.
8. Interpret transmission security models.
9. Name the elements of TEMPEST security.
10. Complete firewall cryptography strategies.
11. Distinguish firewall cryptography strategies.
12. Construct a packet filtering firewall.
13. Implement a proxy server.

CSEC2210 - Security Breaches and Countermeasures

1. Describe threats to and vulnerabilities of systems.
2. Perform risk management functions.
3. Plan a security assessment using current practices.
4. Perform a security assessment using current practices.
5. Utilize current tools to assess network security.
6. Conduct a penetration test using current practices.
7. Employ information reconnaissance techniques.
8. Conduct an IT audit using current best practices.
9. Implement countermeasures for networks.
10. Complete written documentation of threats.
11. Evaluate methods of non-network methods to gain network access.
12. Analyze methods used by attackers to avoid detection.
13. Conduct attacks on a controlled network.
14. Demonstrate ethical behavior.