



CIS Standards

(Updated November 2016)

Cybersecurity for all Programs of Study

Please select the Cybersecurity standards that match the program of study to make sure you have the correct standard reference number.

Page 2 – IT Operations Management Program of Study
Page 3 – Software Development Program of Study

Cybersecurity

Course Description

Cybersecurity introduces the tools and concepts of cybersecurity and encourages students to create solutions that allow people to share computing resources while protecting privacy. Students will solve problems by understanding and closing these vulnerabilities. This course raises students' knowledge of and commitment to ethical computing behavior.

Course Code: 270707

Endorsements to teach: IT

Programs of Study to which this Course applies:

IT Operations Management and Software Development

CIS. HS. 5. 20.

Investigate the application and development of cryptography and cryptanalysis.

- CIS. HS. 5. 20. *a* Identify the real risk of insufficient transport layer protection between wireless devices.
- CIS. HS. 5. 20. *b* Investigate historical cryptography such as the evolution of encryption and ciphers.
- CIS. HS. 5. 20. *c* Explain the social function and mechanics behind public key encryption.
- CIS. HS. 5. 20. *d* Create a cipher that will be used to encrypt information and decrypt encrypted information.
- CIS. HS. 5. 20. *e* Compare and contrast modern cryptographic techniques used to protect information in industry and government.

CIS. HS. 5. 21

Discover the difference between and simple mechanics behind both host-based exploits and network-based vulnerabilities.

- CIS. HS. 5. 21. *a* Employ penetration testing techniques to identify security holes.
- CIS. HS. 5. 21. *b* Identify system vulnerabilities, exploits, and payloads.
- CIS. HS. 5. 21. *c* Discover and implement specific countermeasures for exploits and vulnerabilities.
- CIS. HS. 5. 21. *d* Understand the implications of system vulnerabilities, exploits, and payloads on a network.

CIS. HS. 5. 22

Learn the difference between and common remedies for various malware and viruses.

- CIS. HS. 5. 22. *a* Identify the differences between spyware, bloatware, trojans, worms, adware, ransomware, scareware, and rootkits.
- CIS. HS. 5. 22. *b* Discover how to rectify various common examples of malware and viruses.
- CIS. HS. 5. 22. *c* Demonstrate acute awareness of virus protection techniques.
- CIS. HS. 5. 22. *d* Identify types and capabilities of popular virus protection software.
- CIS. HS. 5. 22. *e* Identify how to avoid spyware, adware, and malware.

CIS. HS. 5. 23.

Employ problem-based learning to explore the extensions of the cybersecurity industry.

- CIS. HS. 5. 23. *a* Solve problems based on reversing, cryptography, forensics, website structures, binary, and computer science trivia.
- CIS. HS. 5. 23. *b* Create problems with solvable solutions based on reversing, cryptography, forensics, website structures, binary, and computing trivia.

CIS. HS. 5. 24

Summarize Internet security issues and remedies.

- CIS. HS. 5. 24. *a* Describe the domains and subdomains of the DNS hierarchy tree.
- CIS. HS. 5. 24. *b* List elements of DNS (e.g., zones, server types).
- CIS. HS. 5. 24. *c* Identify vulnerable TCP and UDP ports such as UDP ports left open for LAN gaming and Telnet.
- CIS. HS. 5. 24. *d* Identify port 22 vulnerabilities.
- CIS. HS. 5. 24. *e* Identify evidence of an SSH (secure shell) service running on a server which, can sometimes be brute forced.

Cybersecurity

Course Description

Cybersecurity introduces the tools and concepts of cybersecurity and encourages students to create solutions that allow people to share computing resources while protecting privacy. Students will solve problems by understanding and closing these vulnerabilities. This course raises students' knowledge of and commitment to ethical computing behavior.

Course Code: 270707

Endorsements to teach: IT

Programs of Study to which this Course applies:

IT Operations Management and Software Development

CIS. HS. 9. 9.

Investigate the application and development of cryptography and cryptanalysis.

- CIS. HS. 9. 9. *a* Identify the real risk of insufficient transport layer protection between wireless devices.
- CIS. HS. 9. 9. *b* Investigate historical cryptography such as the evolution of encryption and ciphers.
- CIS. HS. 9. 9. *c* Explain the social function and mechanics behind public key encryption.
- CIS. HS. 9. 9. *d* Create a cipher that will be used to encrypt information and decrypt encrypted information.
- CIS. HS. 9. 9. *e* Compare and contrast modern cryptographic techniques used to protect information in industry and government.

CIS. HS. 9. 10

Discover the difference between and simple mechanics behind both host-based exploits and network-based vulnerabilities.

- CIS. HS. 9. 10. *a* Employ penetration testing techniques to identify security holes.
- CIS. HS. 9. 10. *b* Identify system vulnerabilities, exploits, and payloads.
- CIS. HS. 9. 10. *c* Discover and implement specific countermeasures for exploits and vulnerabilities.
- CIS. HS. 9. 10. *d* Understand the implications of system vulnerabilities, exploits, and payloads on a network.

CIS. HS. 9. 11

Learn the difference between and common remedies for various malware and viruses.

- CIS. HS. 9. 11. *a* Identify the differences between spyware, bloatware, trojans, worms, adware, ransomware, scareware, and rootkits.
- CIS. HS. 9. 11. *b* Discover how to rectify various common examples of malware and viruses.
- CIS. HS. 9. 11. *c* Demonstrate acute awareness of virus protection techniques.
- CIS. HS. 9. 11. *d* Identify types and capabilities of popular virus protection software.
- CIS. HS. 9. 11. *e* Identify how to avoid spyware, adware, and malware.

CIS. HS. 9. 12.

Employ problem-based learning to explore the extensions of the cybersecurity industry.

- CIS. HS. 9. 12. *a* Solve problems based on reversing, cryptography, forensics, website structures, binary, and computer science trivia.
- CIS. HS. 9. 12. *b* Create problems with solvable solutions based on reversing, cryptography, forensics, website structures, binary, and computing trivia.

CIS. HS. 9. 13

Summarize Internet security issues and remedies.

- CIS. HS. 9. 13. *a* Describe the domains and subdomains of the DNS hierarchy tree.
- CIS. HS. 9. 13. *b* List elements of DNS (e.g., zones, server types).
- CIS. HS. 9. 13. *c* Identify vulnerable TCP and UDP ports such as UDP ports left open for LAN gaming and Telnet.
- CIS. HS. 9. 13. *d* Identify port 22 vulnerabilities.
- CIS. HS. 9. 13. *e* Identify evidence of an SSH (secure shell) service running on a sever which, can sometimes be brute forced.