SYLLABUS

DATE OF LAST REVIEW: 02/2013
CIP CODE: 47.0101
SEMESTER: DEPARTMENTAL SYLLABUS
COURSE TITLE: Security for PC Technicians
COURSE NUMBER: CRTE0114
CREDIT HOURS: 3
INSTRUCTOR: DEPARTMENTAL SYLLABUS
OFFICE LOCATION: DEPARTMENTAL SYLLABUS
OFFICE HOURS: DEPARTMENTAL SYLLABUS
TELEPHONE: DEPARTMENTAL SYLLABUS
EMAIL: KCKCC issued email accounts are the official means for electronically communicating with our students.

PREREQUISITE(S): CRT-0112 Networking for PC Technicians

REQUIRED TEXT AND MATERIALS:

Please check with the KCKCC bookstore, http://www.kckccbookstore.com/, for the required texts for your particular class.

COURSE DESCRIPTION:
This class focus's on the technicians need to understand computer and network security. Failure to implement proper security procedures can have an impact on users, computers, and the general public. Private information, company secrets, financial data, computer equipment, and items of national security are placed at risk if proper security procedures are not followed. After completing this chapter, you will meet these objectives: Explain why security is important. Describe security threats. Identify security procedures. Identify common preventive maintenance techniques for security. Troubleshoot security.
METHOD OF INSTRUCTION: A variety of instructional methods may be used depending on content area. These include but are not limited to: lecture, multimedia, cooperative/collaborative learning, labs and demonstrations, projects and presentations, speeches, debates, and panels, conferencing, performances, and learning experiences outside the classroom. Methodology will be selected to best meet student needs.

COURSE OUTLINE:

I. Explain why security is important

II. Describe security threats
   A. Define viruses, worms, and Trojans
   B. Explain web security
   C. Define adware, spyware, and grayware
   D. Explain Denial of Service
   E. Describe spam and popup windows
   F. Explain social engineering
   G. Explain TCP/IP attacks
   H. Explain hardware deconstruction and recycling

III. Identify security procedures
   A. Explain what is required in a basic local security policy
   B. Explain the tasks required to protect physical equipment
   C. Describe ways to protect data
   D. Describe wireless security techniques

IV. Identify common preventive maintenance techniques for security
   A. Explain how to update signature files for anti-virus and anti-spyware software
   B. Explain how to install operating systems service packs and security patches

V. Troubleshoot security
   A. Review the troubleshooting process
   B. Identify common problems and solutions

VI. Outline security requirements based on customer needs
   A. Outline a local security policy
   B. Explain when and how to use security hardware
   C. Explain when and how to use security application software

VII. Select security components based on customer needs
   A. Describe and compare security techniques
   B. Describe and compare access control devices
   C. Describe and compare firewall types

VIII. Implement customer's security policy
   A. Configure security settings
   B. Describe configuring firewall types
   C. Describe protection against malicious software

IX. Perform preventive maintenance on security
   A. Describe the configuration of operating system updates
   B. Maintain accounts
   C. Explain data backup procedures, access to backups, and secure physical backup
media

X. Troubleshoot security
   A. Review the troubleshooting process
   B. Identify common problems and solutions
   C. Apply troubleshooting skills
   D. Remote Technician: Fix a Security Problem

EXPECTED LEARNER OUTCOMES:
A. The learner will be able to explain why security is important
B. The learner will be able to describe security threats
C. The learner will be able to identify security procedures
D. The learner will be able to identify common preventive maintenance techniques for security
E. The learner will be able to troubleshoot security
F. The learner will be able to explain how to outline security requirements based on customer needs
G. The learner will be able to demonstrate how to select security components based on customer needs
H. The learner will be able to demonstrate how to implement a customers security policy
I. The learner will be able to explain updating for security measures
J. The learner will be able to demonstrate how to troubleshoot security issues

COURSE COMPETENCIES:
   The learner will be able to explain why security is important
1. The learner will be able to discuss why security is important.

   The learner will be able to describe security threats.
2. The learner will be able to define viruses, worms, and Trojans.
3. The learner will be able to explain web security.
4. The learner will be able to define adware, spyware, and grayware.
5. The learner will be able to explain Denial of Service.
6. The learner will be able to describe spam and popup windows.
7. The learner will be able to explain social engineering.
8. The learner will be able to explain TCP/IP attacks.
9. The learner will be able to explain hardware deconstruction and recycling.

   The learner will be able to identify security procedures.
10. The learner will be able to explain what is required in a basic local security policy.
11. The learner will be able to explain the tasks required to protect physical equipment.
12. The learner will be able to describe ways to protect data.

   The learner will be able to identify common preventive maintenance techniques for security.
13. The learner will be able to explain how to update signature files for anti-virus and anti-spyware software.
14. The learner will be able to explain how to install operating systems service packs and security patches.
The learner will be able to troubleshoot security.

15. The learner will be able to review the troubleshooting process.
16. The learner will be able to identify common problems and solutions.

The learner will be able to explain how to outline security requirements based on customer needs.

17. The learner will be able to outline a local security policy
18. The learner will be able to explain when and how to use security hardware
19. The learner will be able to explain when and how to use security application software

The learner will be able to demonstrate how to select security components based on customer needs

20. The learner will be able to describe and compare security techniques
21. The learner will be able to describe and compare access control devices
22. The learner will be able to describe and compare firewall types

The learner will be able to demonstrate how to implement a customer’s security policy

23. The learner will be able to configure security settings
24. The learner will be able to describe configuring firewall types
25. The learner will be able to describe protection against malicious software

The learner will be able to explain updating for security measures

26. The learner will be able to describe the configuration of operating system updates
27. The learner will be able to maintain accounts
28. The learner will be able to explain data backup procedures, access to backups, and secure physical backup media

The learner will be able to demonstrate how to troubleshoot security issues

29. The learner will be able to review the troubleshooting process
30. The learner will be able to identify common problems and solutions
31. The learner will be able to apply troubleshooting skills
32. The learner will be able to remotely fix a Security Problem

ASSESSMENT OF LEARNER OUTCOMES:
Student progress is evaluated by means that include, but are not limited to, exams, written assignments, and class participation.

SPECIAL NOTES:
This syllabus is subject to change at the discretion of the instructor. Material included is intended to provide an outline of the course and rules that the instructor will adhere to in evaluating the student’s progress. However, this syllabus is not intended to be a legal contract. Questions regarding the syllabus are welcome any time.
Kansas City Kansas Community College is committed to an appreciation of diversity with respect for the differences among the diverse groups comprising our students, faculty, and staff that is free of bigotry and discrimination. Kansas City Kansas Community College is committed to providing a multicultural education and environment that reflects and respects diversity and that seeks to increase understanding.

Kansas City Kansas Community College offers equal educational opportunity to all students as well as serving as an equal opportunity employer for all personnel. Various laws, including Title IX of the Educational Amendments of 1972, require the college’s policy on non-discrimination be administered without regard to race, color, age, sex, religion, national origin, physical handicap, or veteran status and that such policy be made known.

Kansas City Kansas Community College complies with the Americans with Disabilities Act. If you need accommodations due to a documented disability, please contact the Director of the Academic Resource Center in Rm. 3354 or call (913) 288-7670.