PURPOSE: The IST Program consists of a number of career studies options that focus on a specific career field in information technology (IT). These programs are appropriate for students earning the IST degree as a means of satisfying the IT electives to obtain a specialized, focus area of expertise.

The career studies certificates listed here provide students with opportunities to gain skills in designing, installing, administering and repairing computer networks; and to explore the various aspects of cyber security.

Before entering a career studies program, students should have a strong foundation in using computer applications (ITE 115 course description in the back of this catalog). Students should also have a strong foundation in computer concepts to include database fundamentals, Internet and networking fundamentals, operating systems, software design and computer hardware troubleshooting prior to beginning the program.

To satisfy the IST degree requirements, students are encouraged to attain competencies within the career studies certificates. Students must also formally complete an "Application for Graduation" for both the Career Studies Certificates and the degree upon attainment of the competencies required for the CSC and the degree upon graduation. The competencies in the Career Studies Certificate programs are directly related to the IST degree.

COMPETENCIES: The following competencies are required for completion of this direct assessment, competency-based education program:

AREA: Cyber Security

I. Network Concepts

1. Carry out basic computer network troubleshooting techniques
2. Carry out trouble-shooting strategies for resolving an identified end-user IT problem.
3. Demonstrate the techniques of defensive programming and secure coding
4. Describe the attitudes, knowledge and abilities associated with quality customer service
5. Describe the layers, protocols, and components of the OSI model
6. Diagram the components of an integrated IT system
7. Differentiate among data types, data transfer protocols and file characteristics specified to the targeted use
8. Differentiate among strategies for business continuity provisioning of IT resources at the enterprise level
9. Differentiate among various computer networking models
10. Differentiate among various techniques for making a computer network secure
11. Discuss significant trends and emerging technologies nd their impact on our global society
12. Explain the process of authentication and authorization between end-user devices and computing network resources
13. Identify a variety of enterprise-level digital storage technologies
14. Implement a hardware and software configuration responsive to an identified scenario
15. Summarize the flow of data through a computer network scenario
16. Summarize the implications of various cloud computing models
17. Summarize the security implications and risk for distributed IT systems
18. Summarize the tenets of ethics and professional behavior promoted by international computing societies
19. Use a variety of practices for making end-user systems secure

II. Network Security Basics

1. Carry out basic computer network troubleshooting techniques on a security related issue.
2. Describe the data management activities associated with the data lifecycle from a security perspective.
3. Diagram the components of an integrated IT system used to exercise good security.
4. Differentiate among data types, data transfer protocols and file characteristics specific to the targeted use. (In this case secured transfers.)
5. Differentiate among strategies for business continuity provisioning of IT resources at the enterprise level.
6. Differentiate among various techniques for making a computer network secure.
7. Differentiate between public and private data.
8. Explain the process of authentication and authorization between end-user devices and computing network resources.
9. Implement a hardware and software configuration responsive to an identified scenario.
10. Modify a system to improve data confidentiality or regulatory compliance.
11. Summarize the security implications and risks for distributed IT systems.
12. Summarize the tenets of ethics and professional behavior promoted by international computing societies.
13. Use a variety of practices for making end-user systems secure.

III. Attacks and Crimes

1. Demonstrate professional behavior in response to an ethically challenging scenario in computing.
2. Describe the layers, protocols and components of the OSI model.
3. Summarize the flow of data through a computer network scenario.
4. Summarize the security implications and risks for distributed IT systems.
5. Summarize the tenets of ethics and professional behavior promoted by international computing societies.
6. Use a programming or a scripting language to share data across an integrated IT system.
7. Use documentation or a knowledge base to resolve a technical challenge in an identified computing scenario.

IV. Access and Authentication

1. Differentiate between public and private data.
2. Explain the process of authentication and authorization between end user devices and computing network resources.
3. Modify a system to improve data confidentiality or regulatory compliance.
4. Summarize the flow of data through a computer network scenario.
5. Use a variety of practices for making end user systems secure.
6. Use documentation or a knowledge base to resolve a technical challenge in an identified computing scenario.

V. Firewalls and E-Commerce

1. Differentiate among various techniques for making a computer network secure.
2. Modify a system to improve data confidentiality or regulatory compliance.
3. Use documentation or a knowledge base to resolve a technical challenge in an identified computing scenario.

VI. Network Security Layers

1. Differentiate among strategies for business continuity provisioning of IT resources at the enterprise level.
2. Differentiate among various techniques for making a computer network secure.
3. Implement a hardware and software configuration responsive to an identified scenario.
4. Modify a system to improve data confidentiality or regulatory compliance.
5. Summarize the security implications and risks for distributed IT systems.
6. Use documentation or a knowledge base to resolve a technical challenge in an identified computing scenario.

VII. Legal Topics

1. Demonstrate professional behavior in response to an ethically challenging scenario in computing.
2. Modify a system to improve data confidentiality or regulatory compliance.
3. Summarize the security implications and risks for distributed IT systems.
4. Use documentation or a knowledge base to resolve a technical challenge in an identified computing scenario

AREA: Networking Specialist

I. Network Concepts

1. Carry out basic computer network troubleshooting techniques
2. Carry out trouble-shooting strategies for resolving an identified end-user IT problem.
3. Demonstrate the techniques of defensive programming and secure coding
4. Describe the attitudes, knowledge and abilities associated with quality customer service
5. Describe the layers, protocols, and components of the OSI model
6. Diagram the components of an integrated IT system
7. Differentiate among data types, data transfer protocols and file characteristics specified to the targeted use
8. Differentiate among strategies for business continuity provisioning of IT resources at the enterprise level
9. Differentiate among various computer networking models
10. Differentiate among various techniques for making a computer network secure
11. Discuss significant trends and emerging technologies nd their impact on our global society
12. Explain the process of authentication and authorization between end-user devices and computing network resources
13. Identify a variety of enterprise-level digital storage technologies
14. Implement a hardware and software configuration responsive to an identified scenario
15. Summarize the flow of data through a computer network scenario
16. Summarize the implications of various cloud computing models
17. Summarize the security implications and risk for distributed IT systems
18. Summarize the tenets of ethics and professional behavior promoted by international computing societies
19. Use a variety of practices for making end-user systems secure

II. Microcomputer OS

1. Carry out trouble-shooting strategies for resolving an identified end-user IT problem.
2. Describe the attitudes, knowledge and abilities associated with quality customer service.
3. Differentiate among various operating systems.
4. Explain the process of authentication and authorization between end-user devices and computing network resources.
5. Implement an application of virtualization.
6. Summarize the tenets of ethics and professional behavior promoted by international computing societies
7. Use a variety of practices for making end-user systems secure.
8. Use communication, negotiation, and collaboration skills as a member of a diverse team.
9. Use documentation or a knowledge base to resolve a technical challenge in an identified computing scenario.

III. PCs and Troubleshooting

1. Carry out trouble-shooting strategies for resolving an identified end-user IT problem.
2. Describe the attitudes, knowledge and abilities associated with quality customer service.
3. Identify basic components of an end-user IT system.
4. Summarize the tenets of ethics and professional behavior promoted by international computing societies.
5. Use documentation or a knowledge base to resolve a technical challenge in an identified computing scenario.

IV. Linux OS

1. Demonstrate the techniques of defensive programming and secure coding.
2. Implement an application of virtualization.

V. Network Administration

1. Differentiate among various operating systems.
2. Differentiate among various techniques for making a computer network secure.
3. Identify a variety of enterprise-level digital storage technologies.

VI. Network Security Basics

1. Carry out basic computer network troubleshooting techniques on a security related issue.
2. Describe the data management activities associated with the data lifecycle from a security perspective.
3. Diagram the components of an integrated IT system used to exercise good security.
4. Differentiate among data types, data transfer protocols and file characteristics specific to the targeted use. (In this case secured transfers.)
5. Differentiate among strategies for business continuity provisioning of IT resources at the enterprise level.
6. Differentiate among various techniques for making a computer network secure.
7. Differentiate between public and private data.
8. Explain the process of authentication and authorization between end-user devices and computing network resources.
9. Implement a hardware and software configuration responsive to an identified scenario.
10. Modify a system to improve data confidentiality or regulatory compliance.
11. Summarize the security implications and risks for distributed IT systems.
12. Summarize the tenets of ethics and professional behavior promoted by international computing societies.
13. Use a variety of practices for making end-user systems secure.