*Business Division*

**CYBERSECURITY**

The program provides preparation for students to obtain entry-level positions in the field of cybersecurity and computer crime deterrence. It also provides preparation and assistance to students for successful transfer to other institutions of higher education. It provides essential skills required to gain and to maintain employment at entry level positions as computer crime investigators, computer security specialists, and federal law enforcement officers. This new program combines elements of both NVCC’s Criminal Justice and Computer Information Systems programs to offer students a strong grounding in understanding the investigative nature of cybersecurity in the criminal justice realm as well as gaining technical skills in computer science networking and programming.

*General Education Core course listings and definitions appear on pages 53-54. Placement testing will determine the sequencing of courses. Additional courses may be required.*

|  |  |  |
| --- | --- | --- |
| **Competency or Program Requirement** | **Course Number and Title** | Required Credits |
| Aesthetic Dimensions/Written  Communications | Choose any Aesthetic Dimensions/  Written Communications listed | 3 |
| Continuing Learning and Information  Literacy/Ethics | CSC\*H101 Introduction to Computers | 3 |
| Critical Analysis and Logical Thinking/  Written Communication | ENG\*101 Composition | 3 |
| Historical Knowledge | BBG\*H231 Business Law | 3 |
| Oral Communication | Choose any Oral  Communications listed | 3 |
| Quantitative Reasoning | MAT\*167 Principles of Statistics1 | 3 |
| Scientific Knowledge◊ | Choose any Scientific Knowledge listed | 4 |
| Scientific Reasoning | CSC\*H252 Information Systems Project Management | 3 |
| Social Phenomena | PSY\*H111 General Psychology I | 3 |
| Written Communication | Choose any Written  Communication listed | 3 |
| Program Requirements | CST\*H130 Network Essentials I | 3 |
| CST\*H274 Network Security and Technology | 3 |
| CST\*H120 Introduction to Operating  Systems or CSC Elective  Any Programming, Operating Systems,  Networking or Database course | 3 |
| FTA\*H272 Terrorism, First  Responders or CST or CSC Elective  Any Programming, Operating Systems,  Networking or Database course | 3 |
| PSY\*H217 Psychology of Criminal Behavior | 3 |
| CST\*H248 Practices in Security Management | 3 |
| CJS\*H101 Introduction to Criminal Justice | 3 |
| CJS\*H224 Computer Crimes | 3 |
| CJS\*H234 Computer Security and Data Protection | 3 |
| CJS\*H235 Information Warfare and Security | 3 |

**Total Credits: 61**

*Any given course may only be used to satisfy one of the competency areas even if it is listed under more than one.*

1 Students planning to transfer to a 4-year school should plan to complete MAT\*H167 Principles of Statistics or MAT\*H172 College Algebra.

◊ Scientific Knowledge must have a lab component.

|  |
| --- |
| ***Program Outcomes*** |

*Upon successful completion of all program requirements, graduates will be able to:*

1. Explain the landscape, key terms, challenges and concepts related to the many layers of cybersecurity. Methodologies include quizzes, tests, written work, and presentations.
2. Explain fundamental architectures of networks (networks build on each other) and demonstrate an understanding of network security. Methodologies include quizzes, tests, written work, presentations, and case studies.
3. Demonstrate an understanding of the legal and ethical issues and concepts associated with cybersecurity responsibilities. Methodologies include exams, quizzes, and written work.

***Associate***

***Degree***

***Programs***

1. Effectively communicate technical information and approaches for incident analysis and response verbally, in writing, and in presentations. Methodologies include written work and presentations.
2. Determine if and when criminal charges will be initiated for different security breaches. Analyze range of security breaches and identify if/when criminal charges are appropriate. Methodologies: case studies.
3. Apply counter measures that would secure network systems against threats. Methodologies: case studies.
4. Identify and discuss career opportunities and the necessary skills that will increase the likelihood of success in the field of cybersecurity, e.g., technical skills, network certifications, interpersonal communications, critical thinking, and leadership skills. Methodologies include presentations and case studies.