

# Secure Systems Administration and Engineering

## Program Information

The job outlook for careers in Cybersecurity and Information Technology continues to be very strong. Many experts predict a continued shortage of qualified professionals available to fill open positions in coming years. Blue River is the host to MCC's Cybersecurity program and home to the Secure Systems Administration and Engineering AAS Degree. Built around stackable certificates mapped to industry certifications, this program helps students earn credentials more quickly, and offers credit by certification for students already holding credentials and wishing to complete a degree or certificate. This program prepares students to enter the in-demand Information Technology and Cybersecurity fields by offering a program that blends current system administration concepts with essential security skills and best practices necessary to deploy, administer, harden, and defend computer and network systems.

MCC is a CompTIA Authorized Academy Partner as well as a VMware Academic Partner. The knowledge and skills gained through our rigorous and hands-on courses will help students earn a degree or certificate while preparing for industry certifications such as:



### **FAQ: What is Cybersecurity?**

**A:** Cybersecurity, also known as Information Security, is information security as applied to computers and computer networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Cybersecurity also includes protection from unplanned events and natural disasters.

The National Initiative for Cybersecurity Education (NICE) has developed a national workforce framework to help identify and organize job roles, as well as to help focus students on a particular path. The NICE workforce framework is broken down into 7 major categories.

The Secure Systems Administration and Engineering program focuses on several roles under the Operate and Maintain and Protect and Defend categories:

### **Category: Operate and Maintain**

Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

#### **Roles:**

- **Customer Service and Technical Support**

Revised 2/16/18

Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support). Typically provides initial incident information to the Incident Response (IR) Specialty.

- **Network Services**

Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

- **Systems Administration**

Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

## **Category: Protect and Defend**

Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.

### **Roles:**

- **Cyber Defense Infrastructure Support**

Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.

More information on NICE framework categories can be found here:

<https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework>

## **Program Structure**

The AAS Secure Systems Administration core is broken down into three stackable Certificates:

- Computer and User Support Certificate
- Network and Systems Support Certificate
- Secure Systems Administration and Engineering Certificate

The certificates are stackable and require completion of the requirements of any lower level certificates before earning a higher-level certificate. For example, a student can complete the Computer and User Support Certificate independently, but it must be completed in addition to the requirements for the next highest-level certificate in order to earn the next level. To earn the Network and Systems Support Certificate, the Computer and User Support Certificate must be completed first. The Secure Systems Administration and Engineering Certificate requires completion of each of the certificates before it, including the new requirements for that certificate, or in other words the entire core.

In addition to completing the course requirements, students must also pass the associated certification exam/s in order to earn the certificate. A course fee is built into several of the courses which will cover the cost of the exam vouchers. Students may choose to take certification exams whenever they are ready,

Revised 2/16/18

generally after the end of the course. Currently, the CompTIA certification exams are not used as the final exams for most courses.

It is possible to complete the core requirements for the degree and not earn the certificates. This would be the result of not passing, or choosing not to take the CompTIA certification exams along the way. Regardless of the individual certificates earned, the degree itself requires sitting for the CompTIA Security+ Exam as part of the capstone course, CSIS 290.

### Secure Systems Administration and Engineering Core

COLL 100	First Year Seminar	1
BSAD 221	Business Communications	3
CSIS 110	Information Technology Fundamentals	3
CSIS 115	Computer Concepts and Applications	3
CSIS 111	Computer Hardware, Maintenance, and Troubleshooting	3
CSIS 151	Microsoft Operating System Concepts	3
		<b>Total</b>
		<b>16</b>
<b>Computer and User Support Certificate</b>		<b>*CompTIA A+</b>

CSIS 123	Programming Fundamentals	3
CSIS 143	Database Design and Management	3
CSIS 152	Linux Operating System	3
CSIS 161	Networking Fundamentals	3
CSIS 172	Windows Server and Active Directory Fundamentals	3
CSIS 174	Virtualization and Cloud Computing Concepts	4
		<b>Total</b>
		<b>19</b>
<b>Network and Systems Support Certificate</b>		<b>*CompTIA Network+</b>

CSIS 170	Principles of Information Assurance	3
CSIS 178	Network and Systems Security	3
CSIS 290	Field Competencies and Employment Strategies	3
		<b>Total</b>
		<b>9</b>
<b>Secure Systems Administration and Engineering Certificate</b>		<b>**CompTIA Security +</b>

<b>Total Credits Hours for AAS Degree</b>	<b>62</b>
---	-----------

\* Certification suggested for degree seekers, and required to earn a certificate.

\*\* Sitting for exam required as part of CSIS 290 capstone.

## Course Schedule

Please see the associated 2-year plans. There is a section for Summer start, Fall Start, and Spring start. While all of the on-ground core courses can be taken at Blue River, some are offered at other campuses as well on a rotating schedule. Following the CSIS course suggestions on the Summer Start schedule allows students to take the CSIS courses listed all at Blue River. Some courses are only offered in hybrid or online only formats, while others are offered only on ground. Please note that while some of the lower level courses are offered on multiple campuses and in different time slots, some of the upper level courses may only be offered once a

Revised 2/16/18

year in an evening format. It is important to work with an advisor or CSIS faculty mentor to help plan course selections each semester.

## **Prospective Students:**

Students with no prior experience will benefit from a robust program that starts with very basic skills and continues to build on key technical and professional fundamentals. Students with prior experience and coursework are encouraged to talk with an advisor to see which courses apply to this degree and to check if their earned industry certifications may be applied as credit towards the degree. A list of certifications that are awarded credit by certification is available at:

<http://www.mcckc.edu/computerscience>

Classes are composed of students with various experience levels ranging from students new to the field as well as those already working in the industry who returned to update knowledge and skills.

## **Additional FAQs**

### **Q: What type of work does someone in Cybersecurity do?**

**A:** Information security professionals plan and carry out security measures to protect an organization's computer networks and systems. Their responsibilities are continually expanding as the number of cyber attacks increase. You may work in areas such as Network Security, Enterprise Security Management, Auditing, Penetration Testing, Threat Analysis, Physical Security, Forensics, etc. in a wide range of industries. The following link further describes job categories and roles found within the field of Information Systems and Cybersecurity:

<https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework>

### **Q: What kind of background do I need?**

**A:** Students will come from a variety of backgrounds and have a varying degree of skill levels. Students will benefit from having taken previous technical courses, experience, and/or having a passion or interest in the field. We also have many students changing careers, coming out of military service, non-traditional students coming back, and students who are starting right out of high school.

### **Q: How long will it take to complete?**

**A:** There are several factors that will play into determining how long it will take to complete any program. Prior coursework and certifications can accelerate completion. Students starting the entire program from the beginning can realistically expect the degree to take 2 years to complete attending full time year round. Remember individual certifications can be earned much more quickly, in as little as a semester or so by attending full time.

### **Q: Does earning the certificates mean I'm not getting a Degree?**

**A:** No. Remember that while you earn the stackable certificates, you are also completing the core for the degree. This method simply allows you to earn a credential more quickly than completing the entire degree.

Revised 2/16/18

**Q: Where can I find Salary and Job Outlook Information**

**A:** Salary and job opportunities are very much dependent on region, industry, company size, education level, and experience. The following site can help you find more salary and job outlook information for your desired path.

<http://www.onetonline.org/>

**Q: Are there any local employers looking to hire CSIS graduates?**

**A:** Many local employers hire our graduates. This includes a wide variety of industries and job titles. Many find employment before completing the program.

**Q: Are there any internship opportunities available?**

**A:** While this program does not guarantee an internship, we are working diligently with regional industry partners to identify as many internship opportunities as possible. Some larger companies do offer internships, however it may be necessary to check with them to determine availability and eligibility. One example of such an opportunity is the KCIT apprenticeship program at Cerner. Please see a faculty member or Cerner's website for guidance on finding more information about that program and connecting with a recruiter.

**Q: Does this degree transfer to any 4-year programs?**

**A:** Currently, the A.A.S Secure Systems Administration and Engineering will transfer directly to the University of Central Missouri (UCM), into the B.S. Systems Engineering Technology degree program. For more information on this transfer agreement, please contact an MCC or UCM advisor

Additionally, many of the courses will transfer to other 4-year programs individually. We are continually working to identify transfer opportunities.

---

Metropolitan Community College is a CompTIA Authorized Academy Partner as well as a VMware Academic partner. We have carefully built and maintained this program with advisory board input, in accordance with industry best practices, and to follow current industry certification requirements. Please see the additional information in the packet regarding CompTIA certifications as well as how CompTIA certifications meet DoD Directive 8570 standards.



**For additional information, please contact:**

**Brian Hurley, CISSP**

CSIS Faculty/Cybersecurity Program Coordinator

816-604-6659

brian.hurley@mckc.edu