# Cybersecurity Certificate

The Cybersecurity Certificate at Johnson County Community College prepares students to step into the information security field. They will be responsible for protecting computers, networks, and data from unauthorized access, change, or destruction. Upon completion, students will have strong foundational skills in cyber defense, network security, ethical hacking, digital forensics, and scripting.

(Major Code 4670; CIP Code 11.0901)

Networking & Cybersecurity Program web page (http://www.jccc.edu/academics/credit/networking-cybersecurity/)

## Program Learning Outcomes

Johnson County Community College (JCCC) is committed to offering high-quality affordable programs that focus on developing knowledge and skills conducive to life-long learning. Both the General Education Student Learning Outcomes (https://www.jccc.edu/about/leadership-governance/administration/institutional-effectiveness-branch/outcomes-assessment/learning-outcomes.html) and Institutional Learning Outcomes (https://www.jccc.edu/about/leadership-governance/administration/institutional-effectiveness-branch/outcomes-assessment/institutional-learning-outcomes.html) convey JCCC's approach to programmatic outcomes. Additionally, students who successfully complete the Cybersecurity Certificate from JCCC will be able to:

- Configure and troubleshoot networking technologies, including IP connectivity, IP services, and security fundamentals.
- Install, configure, and maintain device operating systems including Windows and Linux
- Identify, analyze, and mitigate security events and incidents.
- Understand and explain the key concepts and principles of cybersecurity, such as confidentiality, integrity, availability, authentication, authorization, and encryption.
- Apply appropriate security tools and techniques to protect networks, systems, and data from cyber threats, such as malware, phishing, denial-of-service, and unauthorized access, and prepare students to identify, contain, and remediate cybersecurity incidents.
- Effectively communicate in a professional setting to address information security issues, and educate students about legal and ethical considerations related to cybersecurity, including data privacy regulations and responsible disclosure practices.
- Gain hands-on experience in key areas such as network security, ethical hacking, and incident response, preparing students for real-world challenges in cybersecurity.
- Graduate with practical skills and knowledge that align with current industry demands, enabling immediate entry into entry-level positions in cybersecurity.

## Certificate Requirements

### First Semester

| Code | Title | Hours |
|---|---|---|
| IT 120 | CompTIA A+ Core 2 | 3 |
| IT 141 | Introduction to Networks | 3 |
| IT 230 | Linux Fundamentals | 3 |
| **Total Hours** | | **9** |

### Second Semester

| Code | Title | Hours |
|---|---|---|
| IT 150 | Switching, Routing, and Wireless Essentials* | 3 |
| IT 155 | Microsoft Administration Fundamentals* | 3 |
| IT 175 | Cybersecurity Fundamentals* | 3 |
| IT 231 | Linux Administration* | 3 |
| IT 238 | Digital Forensics* | 3 |
| **Total Hours** | | **15** |

## Third Semester

| Code | Title | Hours |
|---|---|---|
| IT 202 | IT Scripting* | 3 |
| IT 239 | Ethical Hacking* | 3 |
| IT 257 | Cybersecurity Operations* | 3 |
| **Total Hours** | | **9** |

**Total Program Hours: 33**

* This course has registration requirements.