# Virginia Western Community College
# ITN 260
# Network Security Basics

## Prerequisites
ITN 154

## Course Description
Provides instruction in the basics of network security in depth. Includes security objectives, security architecture, security models and security layers; risk management, network security policy, and security training. Includes the five security keys, confidentiality integrity, availability, accountability and auditability.

## Semester Credits: 3 Lecture Hours: 3 Lab/Clinical/Internship Hours: 0

## Required Materials

**Textbook:**
TestOut Security Pro Certification

**Other Required Materials:**
None

## Course Outcomes

**At the completion of this course, the student should be able to:**

- Explain challenges of securing information. Define information security and explain why it's important, identify threat actors and defenses, layers of security and the security lifecycle
- Define malware; types and payload. Discuss technology and personal safety including stalking, bullying, sexual exploitation. Understand how locality impacts how laws are applied. Describe social engineering attacks and defenses.
- Define and describe cryptography and basic algorithms (hash, symmetric, asymmetric), explain different attacks and how cryptography is used.
- Implement cryptography, define and describe digital certificates, PKI, transport encryption algorithms. Understand the challenges and failures of common systems.
- Describe various network-based attacks and defenses. Explain how servers are attacked and defended.
- Discuss how network technologies can enhance security. List different network security devices and uses. Describe secure network architectures and how to implement them.

- Show familiarity with network protocols. Apply understanding to the function and implementation of secure network protocols. Explain network security devices and where they should be deployed. Show an understanding of how to analyze data. Explain how to manage and secure network platforms.
- Describe wireless security devices, protocols and use. Discuss various wireless network attacks, vulnerabilities. Explain solutions for securing wireless networks.
- List the steps for securing client devices and locations. Define and describe application security. Give examples of physical security and how to implement them.
- List and compare different types of mobile device. Discuss deployment, risks and mitigation. Discuss how IoT and connected devices of all types increase convenience as well as risk to health and safety.
- Describe different types of authentication and credentialing. Explain single Sign-On, list account management procedures for securing passwords. Discuss risks and mitigations associated with passwords and other credential/authentication systems
- Define access management and list access control modes. Describe how to manage access through account management. List best practices for access control and implementation. Explain different types of identity and access services. Discuss ways we deal with failures in access management and control.
- Discuss how we assess enterprise security posture. Define vulnerability assessment and explain its importance. Contrast vulnerability scanning, and pen testing. Discuss personal and business data privacy and security. Identify risks and mitigations. Explore the internet, examining privacy as it applies to their own information. Students will write and discuss the impact of technology on privacy and the prevailing policies and laws on privacy.
- Describe fault tolerance through redundancy. Define business continuity. Explain different environmental controls. Describe forensics and incident response procedures.
- Describe the concept of risk. Explain how to manage risk. Describe practices for reducing and mitigating risk. Describe common security issues that cause risk.

## Notes to Instructors

- A mid-term and final exam or project should be required
- At least five hands-on labs should be required

ADA Statement (PDF)
Title IX Statement (PDF)