

Start Your Security+ Certification Today!

Prepare For Your Certification Using AgLearn!

CompTIA Security+ is an international certification that demonstrates competency in network security; compliance and operational security; threats and vulnerabilities; application, data, and host security; access control and identity management; and cryptography.

+ [Auditing, Security Policies, and Disaster Recovery](#) (2.5 hours)

Network administrators create security policies, generate audit reports, and prepare disaster recovery contingency plans. This course examines the methods used to secure a network environment through security policies, user education, and resource monitoring.

+ [Authentication Methods](#) (2 hours)

Developing authentication methods to ensure that users are who they claim to be has been a challenge for administrators since shared networking was first introduced. This course introduces you to the concepts of AAA, hashing, multi-factor authentication, Kerberos, and domain security.

+ [Cryptography](#) (2 hours)

The central goal of cryptography is to hide information from others. This course introduces encryption methods using both symmetric and asymmetric encryption techniques, along with trust models, certificates, and algorithms.

+ [Messaging, User, and Role Security](#) (3 hours)

E-mail and instant messaging have taken over from snail mail and memos in the office environment. The challenge is to ensure that these forms of communication are secure and that the identity all parties involved can be confirmed. This course analyzes and demonstrates the methods for securing e-mail and instant messages.

+ [Ports, Protocols, and Network Security](#) (3 hours)

Selecting the correct devices, properly configuring those devices, and placing them in the correct locations to defend against attack is a task every network administrator faces on a daily basis. This course discusses TCP/IP configuration and attack defenses, network devices selection and proper placement, and securing the networking environment.

+ [Public Key Infrastructure and Access Security](#) (3.5 hours)

Modern network environments use key encryption technologies in order to provide security and availability to both employees and customers. This course explores the use of certificate servers and certificates to provide a secure environment both within a network and when dealing with web servers and internet validations.

+ [Risk Analysis, Vulnerability Testing, IDS, and Forensics](#) (1.5 hours)

The use of risk analysis techniques and forensic methodologies has become the backbone of modern IT security. This course looks at modern risk analysis techniques, forensic methodologies, IDS systems and methods to harden network devices and operating systems.

+ [Threat Mitigation](#) (2 hours)

Even the most secure data systems are threatened on a daily basis, providing the challenge to administrators as well as users to maintain security. This course introduces methods used to perform core system maintenance, manage viruses and spyware, secure browser software, and identify and mitigate social engineering threats.

+ [Wi-Fi and Remote Access](#) (2 hours)

Remote access is becoming more and more prevalent in today's working world. Plane trips, hotel stays, and long distance meetings have made the need for wireless networking and wireless security paramount. This course examines wireless security configuration options along with remote access strategies, VPN configurations, and security measures.

+ [TestPrep SY0-201 Security+](#) (1.5 hours)

TestPrep can be taken in either Study or Certification mode. Study mode is designed to maximize learning by not only testing your knowledge of the material, but also by providing additional information on the topics presented. Certification mode is designed to test your knowledge of the material within a structured testing environment, providing valuable feedback at the end of the test.

As with all AgLearn resources, these are available to all USDA employees at no cost to you!