

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.

+ **[Control Fundamentals and Security Threats](#)** (2 hours)

Understanding the types of threats that exist in an IT infrastructure is incredibly important when you are attempting to control access to network assets and secure an internetwork environment. This course examines control types, authentication, authorization, and access control strategies, along with the various types of malware, social engineering and spam/phishing attacks that a network can face.

+ **[Network Protocols, Attacks, and Defenses](#)** (2 hours)

Network security professionals must have a firm understanding of the transport mechanisms and attacks faced by traffic entering and exiting a network environment. This course examines the TCP/IP protocol suite, the OSI model, and the different protocols that operate within the layers of these models. This course also examines various attacks that protocols and ports can face, along with the tools that can be used to detect these attacks.

+ **[Creating Secure Networks and Performing Security Assessments](#)** (2 hours)

Security professionals must be able to create secure networking environments using appropriate tools and techniques while also being able to test existing network environments for security weaknesses. This course examines the use of routers and switches to create a secure environment. This course also examines security assessment techniques and how penetration testing, vulnerability scanning tools, and honeypots can be used to find holes in network security.

+ **[Network and System Security Mechanisms](#)** (2 hours)

Security professionals must understand the hardware and software mechanisms that can be used to secure a network environment. This course examines the different types of firewalls, NIDS and NIPS, proxy servers, all-in-one security appliances, and other mechanisms that can be put in place to make a network environment secure.

+ **[Remote Access and Wireless Security](#)** (1.5 hours)

Security professionals are increasingly being made responsible for securing remote and wireless environments. This course examines different remote access strategies and technologies such as PPP, VPNs, PPTP, L2TP, IPsec, RADIUS, and TACACS.

+ **[Authentication, Biometrics, and Security Controls](#)** (2 hours)

Security mechanisms and account management are important parts of creating a secure networking environment. This course examines different authentication services and protocols along with biometric security mechanisms and other access security mechanisms such as tokens and smart cards.

+ **[Securing the IT Environment](#)** (2 hours)

Securing the networking environment is the most important job role that a Security specialist will perform. This course examines the methods, tools, and applications that can be used to secure the data, mobile devices, and operating systems, as well as how to deploy environmental controls and physical access controls.

+ **[Cryptography and Public Key Infrastructures](#)** (2.5 hours)

Guaranteeing end-to-end security in communication, document, and database infrastructures is incredibly important in internetworking environments. This course examines cryptography and the different algorithms, ciphers and tools that can be used to secure information, and to protect against attack.

+ **[Securing Applications, Virtualized Environments, and Cloud Computing](#)** (2 hours)

Web servers, web applications, virtualization, and cloud computing are becoming standard parts of corporate infrastructures. This course examines the communications standards and protocols that are used in the web server environment, along with the ways to harden web servers and web browsers.

+ **[Business Continuity, Disaster Recovery, Security Training, and Forensics](#)** (2 hours)

Business continuity, disaster recovery, and computer forensics go hand in hand when a security professional trains on ways to create, maintain, and repair network security. This course examines business continuity plans along with risk assessment techniques and the strategies used when creating a risk management process.

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