This course supports the assessments for DEV1. The course covers 6 competencies and represents 3 competency units.

**Introduction**

**Overview**
This course will provide you with the core fundamentals of information technology security. You will learn how to identify security risks and how to apply security policies, strategies, and tools for securing networks and systems.

With the rapid growth of networked systems, both wired and wireless, security breaches are on the rise. Reports of data breaches cause worry about identity theft. Mobile technology has also introduced risks, and the incidents of cybercrime continue to grow at an alarming rate. There is a high demand for security professionals in the private and government sectors.

Upon completion of this course, you will have a solid understanding of security risks and how to apply strategies and policies for securing systems and networks. You will be prepared to build your foundational knowledge and move into higher level coursework for securing information systems and networks.

Watch the following video for an introduction to this course:

*Note: View the video in full screen at 720p for best results.*

**Competencies**
This course provides guidance to help you demonstrate the following 6 competencies:

- **Competency 400.6.1: Security Layers**
  The graduate applies security measures appropriate to the core goals of an information security program.
- **Competency 400.6.2: Operating Systems Security**
  The graduate applies fundamental authentication and authorization methods.
- **Competency 400.6.3: Auditing Policies**
  The graduate applies security auditing methods.
- **Competency 400.6.4: Network Security**
  The graduate selects appropriate network security technologies to secure a network infrastructure from common threats.
- **Competency 400.6.5: Client Security Software**
  The graduate analyzes appropriate methods for securing clients.
- **Competency 400.6.6: Server Security Software**
  The graduate analyzes appropriate methods for securing servers.

**Course Instructor Assistance**
As you prepare to successfully demonstrate competency in this subject, remember that course
instructors stand ready to help you reach your educational goals. As subject matter experts, mentors enjoy and take pride in helping students become reflective learners, problem solvers, and critical thinkers. Course instructors are excited to hear from you and eager to work with you.

Successful students report that working with a course instructor is the key to their success. Course instructors are able to share tips on approaches, tools, and skills that can help you apply the content you’re studying. They also provide guidance in assessment preparation strategies and troubleshoot areas of deficiency. Even if things don’t work out on your first try, course instructors act as a support system to guide you through the revision process. You should expect to work with course instructors for the duration of your coursework, so you are welcome to contact them as soon as you begin. Course instructors are fully committed to your success!

Preparing for Success

The information in this section is provided to detail the resources available for you to use as you complete this course.

Your Learning Resources

The learning resources listed in this section are required to complete the activities in this course. For many resources, WGU has provided automatic access through the course. However, you may need to manually enroll in or independently acquire other resources. Read the full instructions provided to ensure that you have access to all of your resources in a timely manner.

Automatically Enrolled Learning Resources

You will be automatically enrolled at the activity level for the following learning resources. Simply click on the links provided in the activities to access the learning materials.

VitalSource E-Text

The following textbook is available to you as an e-text within this course. You will be directly linked to the specific readings required within the activities that follow.


Note: This e-text is available to you as part of your program tuition and fees, but you may purchase hard copies at your own expense through a retailer of your choice. If you choose to do so, please use the ISBN listed to ensure that you receive the correct edition.

LearnKey

You will use the following learning resource from LearnKey at the end of this course to review any topics as needed:

- MTA Security Fundamentals
IMPORTANT: There are some important items to understand regarding the use of the LearnKey resource, primarily that it functions best with the Firefox browser. It is recommended that you use Firefox as you utilize the LearnKey resource. If you have technical assistance needs regarding this resource, you are invited to use LearnKey’s Tech Support Facts.

Other Learning Resource

You will use the following learning resources for this course.

**Microsoft DreamSpark (formerly MSDN Academic Alliance)**
Access the following instructions for obtaining free Microsoft software:

- Microsoft DreamSpark (formerly called MSDN Academic Alliance)

**Pacing Guide**
The pacing guide suggests a weekly structure to pace your completion of learning activities. It is provided as a suggestion and does not represent a mandatory schedule. Follow the pacing guide carefully to complete the course in the suggested timeframe.

**Week 1**

- In LearnKey, complete Session 1 Pre-Assessment, Session 2 Pre-Assessment, Session 3 Pre-Assessment, and Session 4 Pre-Assessment.
- Watch the videos listed in the course of study in MTA Security Fundamentals Session 1 Training.
- Read Lesson 1 (Understanding Security Layers) in the course text
- Complete the Session 1 Labs and Post-Assessment

**Week 2**

- Watch the videos listed in the course of study in MTA Security Fundamentals Session 2 Training.
- Read Lesson 2 (Authentication, Authorization, and Accounting) in the course text
- Complete the Session 2 Labs and Post-Assessment

**Week 3**

- Watch the videos listed in the course of study in MTA Security Fundamentals Session 3 Training.
- Read Lesson 3 (Understanding Security Policies) in the course text
- Complete the Session 3 Labs and Post-Assessment

**Week 4**

- Watch the videos listed in the course of study in MTA Security Fundamentals Session 4 Training.
- Read Lesson 4 (Understanding Network Security) in the course text
- Complete the Session 4 Labs and Post-Assessment

Week 5

- Watch the videos listed in the course of study in MTA Security Fundamentals Session 5 Training.
- Read Lesson 5 (Protecting the Server and Client) in the course text
- Complete the Session 5 Labs and Post-Assessment
- Complete MeasureUp in Study Mode and MeasureUp in Certification Mode scoring 90% or higher.
- Work through the end of chapter exercises in the course text. Email your Course Instructor for an answer key.
- Ask your mentor to approve your first attempt.

Note: This pacing guide does not replace the course. Please continue to refer to the course for a comprehensive list of the resources and activities.

Microsoft Official Academic Course Text

The textbook covers all objectives covered on the Microsoft Exam 98-367: Security Fundamentals assessment. Before starting a lesson, review the Lesson Skill Matrix to get a sense of topics covered by the lesson. As you proceed through the lesson material, be sure to complete each practice exercise. These are easily identified by the picture of an arrow with a "GET READY" cue. Each lesson has several hands-on practice exercises, giving you a chance to apply the security tools. Each lesson also points out key certification topics to which you should pay close attention.

Lesson 1: Understanding Security Layers

This lesson introduces you to concepts of confidentiality, integrity, and availability. You will get a first look at security risks and how security can be applied in layers.

This topic addresses the following competencies:

- Competency 400.6.1: Security Layers
  The graduate applies security measures appropriate to the core goals of an information security program.
- Competency 400.6.2: Operating Systems Security
  The graduate applies fundamental authentication and authorization methods.
- Competency 400.6.3: Auditing Policies
  The graduate applies security auditing methods.
- Competency 400.6.4: Network Security
  The graduate selects appropriate network security technologies to secure a network infrastructure from common threats.
- Competency 400.6.5: Client Security Software
  The graduate analyzes appropriate methods for securing clients.
● Competency 400.6.6: Server Security Software
  The graduate analyzes appropriate methods for securing servers.

Lesson 1 Reading

Read the following lesson in *MTA Security Fundamentals* and review the corresponding Power Point:

- lesson 1 ("Understanding Security Layers")
- lesson 1: Power Point

Pay close attention to security terms introduced in this lesson. The security risks, strategies, and processes covered in this lesson will be addressed in depth in future lessons.

If you'd like to check out the lesson at a glance, clicking the following link will give you access:

- lesson 1: Overview

Lesson 1 Knowledge Assessment

Complete the Knowledge Assessment and Competency Assessment activities at the end of the following lesson in *MTA Security Fundamentals*:

- lesson 1 ("Understanding Security Layers")

Do not continue until you have answered everything correctly and understand what you missed. Contact the course instructor for help, if needed. The Proficiency Assessment scenarios are optional.

Lesson 2: Authentication, Authorization, and Accounting

This lesson introduces you to using authentication, authorization, and accounting for access control. These are important strategies for security systems and networks.

This topic addresses the following competencies:

- Competency 400.6.1: Security Layers
  The graduate applies security measures appropriate to the core goals of an information security program.
- Competency 400.6.2: Operating Systems Security
  The graduate applies fundamental authentication and authorization methods.
- Competency 400.6.3: Auditing Policies
  The graduate applies security auditing methods.
- Competency 400.6.4: Network Security
  The graduate selects appropriate network security technologies to secure a network infrastructure from common threats.
- Competency 400.6.5: Client Security Software
  The graduate analyzes appropriate methods for securing clients.
- Competency 400.6.6: Server Security Software
The graduate analyzes appropriate methods for securing servers.

**Lesson 2 Reading**

Read the following lesson in *MTA Security Fundamentals* and review the corresponding Power Point:

- lesson 2 ("Authentication, Authorization, and Accounting ")
- lesson2: Power Point

Pay close attention to security terms introduced in this lesson. The security risks, strategies, and processes covered in this lesson will be addressed in depth in future lessons.

This lesson has several hands-on practice exercises that will give you exposure to some of the tools available for securing resources and providing access in a controlled manner to those that are authorized.

If you'd like to check out the lesson at a glance, clicking the following link will give you access:

- lesson 2: Overview

**Lesson 2 Knowledge Assessment**

Complete the Knowledge Assessment and Competency Assessment activities at the end of the following lesson in *MTA Security Fundamentals*:

- lesson 2 ("Authentication, Authorization, and Accounting ")

Do not continue until you have answered everything correctly and understand what you missed. Contact the course instructor for help, if needed. The Proficiency Assessment scenarios are optional.

**Lesson 3: Understanding Security Policies**

A vital strategy for security is the use of passwords. You will take a close look at password policies and risks associated with passwords.

This topic addresses the following competencies:

- Competency 400.6.1: Security Layers
  The graduate applies security measures appropriate to the core goals of an information security program.
- Competency 400.6.2: Operating Systems Security
  The graduate applies fundamental authentication and authorization methods.
- Competency 400.6.3: Auditing Policies
  The graduate applies security auditing methods.
- Competency 400.6.4: Network Security
  The graduate selects appropriate network security technologies to secure a network infrastructure from common threats.
Lesson 3 Reading

Read the following lesson in *MTA Security Fundamentals* and review the corresponding Power Point:

- [lesson 3 ("Understanding Security Policies")](#)
- [lesson3: Power Point](#)

This lesson covers passwords in depth. The hands-on exercises will include an opportunity to use group policy. Using Group Policy Object (GPO) is a key skill required by system administrators.

If you'd like to check out the lesson at a glance, clicking the following link will give you access:

- [lesson 3: Overview](#)

Lesson 3 Knowledge Assessment

Complete the Knowledge Assessment and Competency Assessment activities at the end of the following lesson in *MTA Security Fundamentals*:

- [lesson 3 ("Understanding Security Policies")](#)

Do not continue until you have answered everything correctly and understand what you missed. Contact the course instructor for help, if needed. The Proficiency Assessment scenarios are optional.

**Lesson 4: Understanding Network Security**

This lesson covers all of the basics of wired and wireless security.

This topic addresses the following competencies:

- Competency 400.6.1: Security Layers
  The graduate applies security measures appropriate to the core goals of an information security program.
- Competency 400.6.2: Operating Systems Security
  The graduate applies fundamental authentication and authorization methods.
- Competency 400.6.3: Auditing Policies
  The graduate applies security auditing methods.
- Competency 400.6.4: Network Security
  The graduate selects appropriate network security technologies to secure a network infrastructure from common threats.
- Competency 400.6.5: Client Security Software
The graduate analyzes appropriate methods for securing clients.

- Competency 400.6.6: Server Security Software
  The graduate analyzes appropriate methods for securing servers.

**Lesson 4 Reading**

Read the following lesson in *MTA Security Fundamentals* and review the corresponding Power Point:

- lesson 4 ("Understanding Network Security")
- lesson 4: Power Point

This lesson is one of the most challenging in the text. You will learn about firewalls, Network Access Points, and the basics of protocol security. You will be introduced to the OSI model. Please pay close attention to the purpose of each layer in the OSI model. Using this model of network architecture will help you apply security appropriately.

If you'd like to check out the lesson at a glance, clicking the following link will give you access:

- lesson 4: Overview

**Lesson 4 Knowledge Assessment**

Complete the Knowledge Assessment and Competency Assessment activities at the end of the following lesson in *MTA Security Fundamentals*:

- lesson 4 ("Understanding Network Security")

Do not continue until you have answered everything correctly and understand what you missed. Contact the course instructor for help, if needed. The Proficiency Assessment scenarios are optional.

**Lesson 5: Protecting the Server and Client**

This lesson covers how to protect systems from malware. You may be administrating several users in the future. This chapter will introduce you to the various risks your users will face and strategies for protecting both client systems and servers.

This topic addresses the following competencies:

- Competency 400.6.1: Security Layers
  The graduate applies security measures appropriate to the core goals of an information security program.
- Competency 400.6.2: Operating Systems Security
  The graduate applies fundamental authentication and authorization methods.
- Competency 400.6.3: Auditing Policies
  The graduate applies security auditing methods.
• Competency 400.6.4: Network Security
  The graduate selects appropriate network security technologies to secure a network infrastructure from common threats.
• Competency 400.6.5: Client Security Software
  The graduate analyzes appropriate methods for securing clients.
• Competency 400.6.6: Server Security Software
  The graduate analyzes appropriate methods for securing servers.

Lesson 5 Reading

Read the following lesson in *MTA Security Fundamentals* and review the corresponding Power Point:

- lesson 5 ("Protecting the Server and Client")
- lesson 5: Power Point

As you read this lesson, be sure to complete the practice exercises. You will be given the opportunity to use User Account Control and examine your firewall configuration.

If you'd like to check out the lesson at a glance, clicking the following link will give you access:

- lesson 5: Overview

Lesson 5 Knowledge Assessment

Complete the Knowledge Assessment and Competency Assessment activities at the end of the following lesson in *MTA Security Fundamentals*:

- lesson 5 ("Protecting the Server and Client")

Do not continue until you have answered everything correctly and understand what you missed. Contact the course instructor for help, if needed. The Proficiency Assessment scenarios are optional.

**MeasureUp**

The MeasureUp learning resource is meant to complement the other learning resources for this course.

**MeasureUp Software**
The MeasureUp testing software provides you with the necessary tools to reinforce your learning and validate your knowledge for certification.

This topic addresses the following competencies:

- Competency 400.6.1: Security Layers
  The graduate applies security measures appropriate to the core goals of an information security program.
- Competency 400.6.2: Operating Systems Security
The graduate applies fundamental authentication and authorization methods.

- **Competency 400.6.3: Auditing Policies**
  The graduate applies security auditing methods.

- **Competency 400.6.4: Network Security**
  The graduate selects appropriate network security technologies to secure a network infrastructure from common threats.

- **Competency 400.6.5: Client Security Software**
  The graduate analyzes appropriate methods for securing clients.

- **Competency 400.6.6: Server Security Software**
  The graduate analyzes appropriate methods for securing servers.

**MeasureUp Testing**

Complete the following MeasureUp material:

- **MTA: Security Fundamentals**

Please use the steps listed in following document to guide your study of the MeasureUp material:

- **Using MeasureUp**

**LearnKey**

*This section covers threats and risks, authentication, password policies, auditing, malware protection, encryption basics, network security, wireless security, client and server protection, and e-mail protection.*

**LearnKey MTA Security Fundamentals**

*IMPORTANT: There are some important items to understand regarding the use of the LearnKey resource, primarily that it functions best with the Firefox browser. It is recommended that you use Firefox as you utilize the LearnKey resource. If you have technical assistance needs regarding this resource, you are invited to use LearnKey’s Tech Support Facts.*
Final Steps

Congratulations on completing the activities in this course! This course has prepared you to complete the assessments associated with this course. If you have not already been directed to complete the assessments, schedule and complete your assessments now.

First Attempt Checklist

One of the many things that makes WGU unique is its competency based education model. If you know the material, all you have to do is prove it by passing the exam. If you can do this, you can accelerate the receipt of your degree.

To make sure you have the best chance possible to pass the exam on your first attempt, the following should be completed before you refer to take it:

1. Go through the course in its entirety. Mark as complete as you progress.
2. Read through the entire book and complete all exercises.
3. Complete MeasureUp in Certification Mode and score at least 90% or better on the exam. Recommend doing this multiple times to ensure you are seeing the entire test bank.
4. It is recommended that the student has spent 5-8 weeks studying for their first attempt.

LearnKey is a supplemental resource provided for students who need additional resources for this course. Although recommended, it is not required for the first attempt. To increase your chances on your first attempt, it is highly recommended that in addition to the above checklist, that you complete all 3 sessions within LearnKey to better grasp the competencies of this course.

After completing the above sections and passing, please speak to your program mentor to have your voucher emailed to you.

If the first attempt is failed, you will be required to get in contact with the course instructor to see what went wrong and how you can prepare to make sure your second attempt is a success. Once the course instructor feels you are ready to refer for the second attempt of the exam, he or she will approve your second exam referral.

Outside Vendor Assessment


- View Microsoft's information about this exam on the "Exam 98-367: Security Fundamentals" web page.

Security Fundamentals Exam Referral Instructions

1. Create a Certiport Account

In order to refer for your final exam, you will first need to create an account with Certiport. Click 'Register' and follow the required steps. Please keep your login information handy—you will need
to log into your Certiport account to take your assessment.

2. Choose an Assessment Location
The assessment has to be taken at a proctored site; there are two options for choosing a site:

a. The Certiport website has a network of testing sites from which to choose.

b. If you cannot find a Certiport site that is close to you, you can search for a site in the "WGU Proctor Yellow Pages." This site would have to be set up by Certiport, please follow step 4.2

3. Contact the Certiport Testing Center to Schedule Your Exam

a. Most testing centers listed on the Certiport locator will provide a phone number for you to call and schedule, others will list an e-mail address or have a link to their website. Please use their preferred method to arrange your assessment.

   Please note: Some testing centers require a proctor fee that has to be paid to the site, independent from the voucher number that pays for the exam itself. Check with the site on the amount of the proctor fee and how it can be paid to them.

Once you have a scheduled test date and time, follow step 4.

b. If the testing center will not allow you to make an appointment, please proceed to step 4.3

4. Submit Your Referral

4.1 To complete the scheduling process for an exam on your Degree Plan, click the ‘schedule now’ button for this assessment. You will be required to provide the date and time your exam is scheduled, the name of the testing center, and any proctor fees; please make sure you have this information available.

4.2 If you cannot find a site or found a site in the WGU network that you would like to become a Certiport testing center, click the checkbox next to ‘I need help finding a site’ and enter the name of the WGU site or the reason why you need help scheduling in the notes section underneath. This will cancel the requirement of entering any of the other required information the referral is asking for and will allow you to submit the referral. A scheduler will then work with you to get a site set up for you.

4.3 If the Certiport testing site does not allow you to make an appointment without a voucher number for this assessment, click the checkbox next to ‘I need help finding a site’ and enter in the notes section underneath which site you selected and that they require a voucher number to schedule your appointment.

   IMPORTANT: WGU will provide a discounted Certiport voucher for this assessment and will pay all associated proctor fees. You will receive the voucher within 3 business days of submitting the referral. Please understand that you will only be reimbursed the amount WGU would pay for a
discounted voucher if you purchased a voucher directly from Certiport. However, you will be reimbursed the full amount of any proctor fee the site might charge you if WGU cannot pay the site directly. Submit receipts to reimbursements@wgu.edu along with your current mailing address and the date and exam code and you will receive a check within 3 weeks.

5. Verify Your Information
Make sure you fill out the information as requested before submitting the referral. Double check to make sure everything is correct and in order. Please provide any other information you feel your scheduler needs to know before processing this request for you.

Submitting Outside Vendor Assessment Scores

After completing an outside vendor assessment, follow the directions for submitting a score report on the “Following Outside Vendor Assessments” page.