

**NOTE:**

**COURSE CONTENT MAY BE CHANGED, TERM TO TERM, WITHOUT NOTICE. THE INFORMATION BELOW IS PROVIDED AS A GUIDE FOR COURSE SELECTION AND IS NOT BINDING IN ANY FORM, AND SHOULD NOT BE USED TO PURCHASE COURSE MATERIALS.**

## ***COURSE SYLLABUS***

---

### **CSIS 341**

#### **INFORMATION SECURITY PLANNING**

#### **COURSE DESCRIPTION**

This course will deal with the proper planning for and initial implementation of an Information Security program. The topics included would be: security planning and policies, risk analysis, program accreditation, systems lifecycle management, contingency planning, physical security measures, personal security practices and procedures, software security, network security, administrative controls, crypto security.

#### **RATIONALE**

In order for students to fully grasp information systems security, they must have a thorough understanding of system capabilities, functionality, and how to best protect the system. Operation of a healthy organization requires reliable business processes that protect information, legal compliance, and keep costs low. Properly designed and implemented information security policies and frameworks mitigate risks that increase with the expansion of global interactivity and connectivity. To mitigate these risks, security plans must be implemented, audited, and maintained.

#### **I. PREREQUISITES**

CSIS 340 - For information regarding prerequisites for this course, please refer to the [Academic Course Catalog](#).

#### **II. REQUIRED RESOURCE PURCHASES**

Click on the following link to view the required resource(s) for the term in which you are registered: <http://bookstore.mbsdirect.net/liberty.htm>

#### **III. ADDITIONAL MATERIALS FOR LEARNING**

- A. Computer with a minimum of 20GB of free hard disk space and basic audio/video output equipment
- B. Internet access (broadband recommended)
- C. Microsoft Office

#### **IV. MEASURABLE LEARNING OUTCOMES**

Upon successful completion of this course, the student will be able to:

- A. Evaluate the key components of information security policy planning guidelines.
- B. Evaluate information security policy regulations and framework.
- C. Analyze industry specific sector requirements pertinent to policy development.
- D. Select current business information security policies to obtain best practices.
- E. Apply guidelines and best practices during the development of a security policy.

**V. COURSE REQUIREMENTS AND ASSIGNMENTS**

- A. Textbook readings

- B. Course Requirements Checklist

After reading the Course Syllabus and [Student Expectations](#), the student will complete the related checklist found in Module/Week 1.

- C. Discussion Board Forums (5)

Discussion boards are collaborative learning experiences. Therefore, the student will participate in weekly activities by researching and addressing the topics provided for each module. During the weekly Discussion Board Forum assignments on information security planning, the student will post 1 thread and 2 replies.

- D. Projects (7)

The student will implement practical hands-on learning skills into a virtualized server environment. Each project is intended to deliver a unique learning experience designed to engage the student to apply the theory learned throughout the module/week into a practical research-based learning environment.

In order to utilize this implementation, a minimum of 25 GB of available hard disk space, with at least 512 MB RAM, and running at least an Intel (or equivalent) 1 GHz processor, which supports virtualization technologies, is required. It is recommended that the system consist of a multi-core processor running a 64-bit Operating System environment.

- E. Mid-Term Research Paper (1)

In Module/Week 4, the student is asked to write a paper which provides a comprehensive reflection of the learning objectives and concepts addressed in the course so far.

- F. Final Research Paper (1)

In Module/Week 8, the student will prepare a research paper that is designed to provide a comprehensive learning approach where the student can utilize the information learned throughout the course and apply it in a practical and theoretical manner.

**VI. COURSE GRADING AND POLICIES**

A. Points

Course Requirements Checklist	10
Discussion Board Forums (5 at 25 pts ea)	125
Projects (7 at 50 pts ea)	350
Mid-Term Research Paper (1 at 225 pts)	235
Final Research Paper (1 at 290 pts)	290
<b>Total</b>	<b>1010</b>

B. Scale

A=900-1010 B=800-899 C=700-799 D=600-699 F=0-599

D. Disability Assistance

Students with a documented disability may contact Liberty University Online's Office of Disability Academic Support (ODAS) at [LUOODAS@liberty.edu](mailto:LUOODAS@liberty.edu) to make arrangements for academic accommodations. Further information can be found at [www.liberty.edu/disabilitysupport](http://www.liberty.edu/disabilitysupport).

## ***COURSE SCHEDULE***

### **CSIS 341**

Textbook: Gregory, P.H. (2014). *CISSP Guide To Security Essentials* (2nd ed.). Boston, MA: Cengage Learning.

Walker, M. (2014). *CEH Certified Ethical Hacker Bundle* (2nd ed.). New York, NY: McGraw-Hill Education.

<b>MODULE/ WEEK</b>	<b>READING &amp; STUDY</b>	<b>ASSIGNMENTS</b>	<b>POINTS</b>
<b>1</b>	Gregory: Chapter 1 Walker: Chapter 1 1 presentation 3 websites	Course Requirements Checklist Discussion Board Forum 1 Project 1	10 25 50
<b>2</b>	Gregory: Chapter 2 1 presentation 3 websites	Discussion Board Forum 2 Project 2	25 50
<b>3</b>	Gregory: Chapter 3 3 websites	Discussion Board Forum 3 Project 3	25 50
<b>4</b>	Walker: Chapter 2 & 3 1 presentation 4 websites	Project 4 Mid-Term Research Paper 4	50 235
<b>5</b>	Gregory: Chapter 4 1 presentation 3 websites	Discussion Board Forum 5 Project 5	25 50
<b>6</b>	Gregory: Chapter 6 1 presentation 4 websites	Discussion Board Forum 6 Project 6	25 50
<b>7</b>	Gregory: Chapter 7 1 presentation 4 websites	Project 7	50
<b>8</b>	Gregory: Chapter 8 & 9 1 presentation 3 websites	Final Research Paper	290
<b>TOTAL</b>			<b>1010</b>

**NOTE:** Each course module/week (except Module/Week 1) begins on Tuesday morning at 12:00 a.m. (ET) and ends on Monday night at 11:59 p.m. (ET). The final module/week ends at 11:59 p.m. (ET) on **Friday**.