

Syllabus

Course Title: Fundamentals of E-Security II

Course Number: CN 461

Course Description:

A continuation of CN460. Uses an integrated study of network security, cryptography, operational security, disaster recovery and business continuity planning, and information security legal issues to round out the essential e-security foundation.

Prerequisite Courses:

CN 460 Fundamentals of E-Security I

Course Overview

This course continues the concepts of information security management and addresses the ambient factors that constitute a sound organizational security policy. Examines basic security management, security models, risk analysis, internal and external security threats, privacy issues and security laws and regulations in an effort to provide a solid foundation for future e-security courses.

Key concepts to be covered in this course include:

- Telecommunications and network security
- Cryptography
- Application security
- Operational security
- Business continuity and disaster recovery
- Law and investigations

Course Outcomes:

Upon completion of this course, learners should be able to:

- Understand how telecommunications and network security are related
- Comprehend the different types of cryptography algorithms
- Apply concepts of application security
- Better understand operations security

- Evaluate a business continuity and disaster recovery plan

Course Materials:

Required Texts:

Harris, S. (2012). *CISSP All-in-One Exam Guide* (6th ed.): McGraw-Hill Osborne Media. ISBN 0071781749, 978-0071781749.

American Psychological Association. (2010). *Publication Manual of the American Psychological Association* (6th ed.). Washington, DC: American Psychological Association. ISBN 1433805618, 978-1433805615. Companion website: <http://www.apastyle.org>.

Required Resources:

Grossaint, K. (2001). Essential writing knowledge. Denver, CO: Regis University. Select link for Essential Writing Knowledge.

Technology Tools:

The labs are designed to run either as a live CD or as a virtualized computer using a software package such as VMWare, Parallels, or VirtualBox.

You must have up to date virus protection software on your computer. If your computer does not meet any of these requirements please contact the instructor immediately.

Minimum Requirements for Live CDs

- 800 MHz Intel-based processor
- 1 Gigabyte (GB) RAM

Minimum Requirements for Virtualization

- 1 GHz processor (2 GHz or higher recommended)
- 1 GB RAM (2 GB or higher recommended)
- 10 GB available hard disk space (30 GB recommended)

Cable or DSL Internet connection

- Don't use a modem dial-up connection. This will not work for this course. Dial-up is simply not fast enough for this course.

Pre-Assignment:

1. Read Ch. 6 “Telecommunications and Network Security”, pages. 515 - 657- Harris, S. *All-in-One CISSP Exam Guide 6th Edition*. (2012).
2. Reflect on the following statement in the discussion forum in the context of the Jesuit meaning of “How ought we live”: Statement: I believe ethics are formed in the following ways.

3. Ethics Statement:

Online Format: Read and acknowledge the Regis University Ethics Statement in the discussion forum under the Introduction. Copy the statement at the bottom of the Ethics Statement document and paste it in a reply to the statement inserting your name in the appropriate blanks and the date at the end.

Classroom-based Format: Read and sign the Regis University Ethics Statement provided by your instructor.

4. Online Introductions:

Online Format: Sign on to D2L (Home Page) and become familiar with the course navigation of the Web Curriculum. Post an introduction in the introductions forum by Wednesday night of the first week of class.

Pre-Assignment Due Dates:

Classroom-based Format: This assignment is due the first night of class.

Online Format: The instructor will specify the due date for this assignment.

Course Assignments and Activities:

	Topics	Readings	Activities Assignments and Associated Points
1	Getting Started Telecommunications and Network Security	Text: Chapter 6 Telecommunications and Network Security—up to but not including Intranets and Extranets	Class Discussion: <ul style="list-style-type: none"> • Introductions • Weekly Discussion Forum (25 pts) Written Assignment: <ul style="list-style-type: none"> • Ethics Statement response (25 pts) • Security Entrance Examination (50 pts) • Business Continuity/Disaster Recovery (BCP/DR) Paper -Working Draft (0 pts)
2	Telecommunications and Network Security (continued)	Text: Chapter 6 Telecommunications and Network Security—continuing from Intranets and Extranets to the end of the chapter	Class Discussion: <ul style="list-style-type: none"> • Weekly Discussion Forum (25 pts) Written Assignment: <ul style="list-style-type: none"> • Network Security – Vulnerability Scanning Lab (50 pts)
3	Cryptography	Text: Chapter 7 Cryptography—through Types of Symmetric Systems.	Class Discussion: <ul style="list-style-type: none"> • Weekly Discussion Forum (25 pts) Written Assignment: <ul style="list-style-type: none"> • CrypTool Lab (50 pts)

4	Cryptography (continued)	Text: Chapter 7 Cryptography—from Types of Asymmetric Systems to the end of the chapter.	Class Discussion: <ul style="list-style-type: none"> Weekly Discussion Forum (25 pts) Written Assignment: <ul style="list-style-type: none"> Midterm Paper – Networking and Cryptography (100 pts)
5	Application Security	Text: Chapter 10 Software Development Security	Class Discussion: <ul style="list-style-type: none"> Weekly Discussion Forum (25 pts) Written Assignment: <ul style="list-style-type: none"> Thesis Statement – Course Project Paper LabRat/WebGoat Lab (50 pts)
6	Operations Security	Text: Chapter 11 Security Operations	Class Discussion: <ul style="list-style-type: none"> Weekly Discussion Forum (25 pts) Written Assignment: <ul style="list-style-type: none"> Thesis Statement Due (0 pts)
7	Business Continuity Plan / Disaster Recovery (BCP/DR)	Text: Chapter 8 Business Continuity and Disaster Recovery Planning	Class Discussion: <ul style="list-style-type: none"> Weekly Discussion Forum (25 pts) Written Assignment: <ul style="list-style-type: none"> Course Project: Business Continuity Plan / Disaster Recovery (BCP/DR) Paper and BCP/DR Presentation (200 pts)
8	Laws and Investigations	Text: Chapter 9 Legal, Regulations, Investigations, and Compliance	Class Discussion: <ul style="list-style-type: none"> Weekly Discussion Forum (25 pts) Written Assignment: <ul style="list-style-type: none"> Timely evaluation of two colleagues' BCP/DR Presentations (25 pts) Leadership Points (e.g. Substantive Discussion Forum based upon Discussion Forum Rubric) (50 pts)
			Maximum Points Possible: 800

Course Policies and Procedures:

CC&IS Grading Scale

Letter Grade	Percentage	Grade Point
A	93 to 100	4.00
A–	90 to less than 93	3.67
B+	87 to less than 90	3.33
B	83 to less than 87	3.00
B–	80 to less than 83	2.67
C+	77 to less than 80	2.33
C	73 to less than 77	2.00
C–	70 to less than 73	1.67
D+	67 to less than 70	1.33
D	63 to less than 67	1.00
D-	60 to less than 63	.67
F	Less than 60	0

Additional information about grading can be found in the latest edition of the University Catalog, available at <http://www.regis.edu/Academics/Course%20Catalog.aspx>.

CC&IS Policies and Procedures

Each of the following CC&IS Policies & Procedures is incorporated here by reference. Students are expected to review this information each term, and agree to the policies and procedures as identified here and specified in the latest edition of the University Catalog, available at <http://www.regis.edu/Academics/Course%20Catalog.aspx> or at the link provided.

- The CC&IS Academic Integrity Policy.
- The Student Honor Code and Student Standards of Conduct.
- Incomplete Grade Policy, Pass / No Pass Grades, Grade Reports.
- The Information Privacy policy and FERPA. For more information regarding FERPA, visit the [U.S. Department of Education](http://www.ed.gov).
- The HIPAA policies for protected health information. The complete Regis University HIPAA Privacy & Security policy can be found here: <http://www.regis.edu/About-Regis-University/University-Offices-and-Services/Auxiliary-Business/HIPAA.aspx>.
- The Human Subjects Institutional Review Board (IRB) procedures. More information about the IRB and its processes can be found here: <http://regis.edu/Academics/Academic-Grants/Proposals/Regis-Information/IRB.aspx>.

The CC&IS Policies & Procedures Syllabus Addendum summarizes additional important policies including, Diversity, Equal Access, Disability Services, and Attendance & Participation that apply to every course offered by the College of Computer & Information Sciences at Regis University. A copy of the CC&IS Policies & Procedures Syllabus Addendum can be found here: <https://in2.regis.edu/sites/ccis/policies/Repository/CCIS%20Syllabus%20Addendum.docx>.