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:


Required Resources:

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:

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:**

<table>
<thead>
<tr>
<th></th>
<th>Topics</th>
<th>Readings</th>
<th>Activities Assignments and Associated Points</th>
</tr>
</thead>
</table>
| 1 | Getting Started Telecommunications and Network Security | Text: Chapter 6 Telecommunications and Network Security–up to but not including Intranets and Extranets | Class Discussion:  
   • Introductions  
   • Weekly Discussion Forum (25 pts)  
   Written Assignment:  
   • 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:  
   • Weekly Discussion Forum (25 pts)  
   Written Assignment:  
   • Network Security – Vulnerability Scanning Lab (50 pts) |
| 3 | Cryptography                                | Text: Chapter 7 Cryptography–through Types of Symmetric Systems. | Class Discussion:  
   • Weekly Discussion Forum (25 pts)  
   Written Assignment:  
   • CrypTool Lab (50 pts) |
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Topic</th>
<th>Text: Chapter</th>
<th>Class Discussion:</th>
<th>Written Assignment:</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Cryptography (continued)</td>
<td>Cryptography–from Types of Asymmetric Systems to the end of the chapter.</td>
<td>Weekly Discussion Forum (25 pts)</td>
<td>Midterm Paper – Networking and Cryptography (100 pts)</td>
</tr>
<tr>
<td>6</td>
<td>Operations Security</td>
<td>Chapter 11 Security Operations</td>
<td>Weekly Discussion Forum (25 pts)</td>
<td>Thesis Statement Due (0 pts)</td>
</tr>
<tr>
<td>8</td>
<td>Laws and Investigations</td>
<td>Chapter 9 Legal, Regulations, Investigations, and Compliance</td>
<td>Weekly Discussion Forum (25 pts)</td>
<td>Timely evaluation of two colleagues’ BCP/DR Presentations (25 pts) Leadership Points (e.g. Substantive Discussion Forum based upon Discussion Forum Rubric) (50 pts)</td>
</tr>
</tbody>
</table>

Maximum Points Possible: 800
Course Policies and Procedures:

CC&IS Grading Scale

<table>
<thead>
<tr>
<th>Letter Grade</th>
<th>Percentage</th>
<th>Grade Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>93 to 100</td>
<td>4.00</td>
</tr>
<tr>
<td>A–</td>
<td>90 to less than 93</td>
<td>3.67</td>
</tr>
<tr>
<td>B+</td>
<td>87 to less than 90</td>
<td>3.33</td>
</tr>
<tr>
<td>B</td>
<td>83 to less than 87</td>
<td>3.00</td>
</tr>
<tr>
<td>B–</td>
<td>80 to less than 83</td>
<td>2.67</td>
</tr>
<tr>
<td>C+</td>
<td>77 to less than 80</td>
<td>2.33</td>
</tr>
<tr>
<td>C</td>
<td>73 to less than 77</td>
<td>2.00</td>
</tr>
<tr>
<td>C–</td>
<td>70 to less than 73</td>
<td>1.67</td>
</tr>
<tr>
<td>D+</td>
<td>67 to less than 70</td>
<td>1.33</td>
</tr>
<tr>
<td>D</td>
<td>63 to less than 67</td>
<td>1.00</td>
</tr>
<tr>
<td>D–</td>
<td>60 to less than 63</td>
<td>.67</td>
</tr>
<tr>
<td>F</td>
<td>Less than 60</td>
<td>0</td>
</tr>
</tbody>
</table>

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.
- The HIPPA 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 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.