Syllabus

Course Number: MSIA 673

Course Title: Legal Basics in Cyber and Information Security

Course Description:
Explores laws, regulations, legal issues and trends associated with cyber and information security. Provides security practitioners insight and practical application for identifying and addressing legal issues in all stages of security implementation and practice.

Prerequisite Courses: None

Course Overview:
Welcome to the “Legal Basics in Cyber and Information Security” course (MSIA673). This is a graduate level course focused on providing students insight to the major cyber and information security (InfoSec) laws/regulations, both national and international, a few of the more popular InfoSec best practices/standards and the legal trends developing in the courts and in commentary over major breaches.

The study of these resources will help the student understand the legal landscape with regard to cyber security and InfoSec. It will provide students the knowledge necessary to effectively develop and maintain cyber and information security plans and programs. Finally, students will be much better positioned to understand, define and implement “reasonable security” to protect the organization's they support and are responsible for protecting.

Key concepts to be covered in this course include:
• Introduction to the law related to cyber and information security
• Review and analysis current legal trends in cyber security
• Discussion of what legally constitutes “reasonable security”

Course Outcomes:
Upon completion of this course, learners should be able to:
1. Articulate current and pertinent U.S. and international law related to cyber- security, information security (InfoSec) and privacy and synthesize legal trends with regard to data breaches and cyber security.
   a. Identify and briefly describe major and significant laws related to cyber and InfoSec implementation and practice.
   b. Identify current legal trends in the courts and their potential impact on cyber and InfoSec practice.
2. Recognize and identify legal issues and trends in the full spectrum of an InfoSec program.
   a. Identify legal issues in a current security program.
   b. Identify legal issues during the development of a security program.
3. Demonstrate the ability to incorporate legal, regulatory, policy and compliance rules and issues into the development of a cyber and information security plan, from implementation to incident response, and know when to seek legal assistance.
a. Outline the legal issues in a cyber/InfoSec plan/program and incorporate the law, regulation, policy and compliance, as well as legal trends into this program.
b. Understand when to get the legal advisors involved.
c. Understand how to bridge the gap for lawyers between the law and technology.

Required Texts:
None

Required Readings:
Refer to the Required Readings list in the Course Resources folder for this course in WorldClass. The Readings are assigned by Topic. Note that there is no cost to access any of the Required Readings online.

Technology Tools:

Optional Materials:
None

Pre-Assignment and Due Dates:
- Classroom-based Format: Check with your facilitator.
- Online Format: See Course Assignments and Activities table below for details Week 1.
### Course Assignments and Activities:

<table>
<thead>
<tr>
<th>Topic/Week</th>
<th>Topics</th>
<th>Readings</th>
<th>Assignments</th>
</tr>
</thead>
</table>
| 1          | Overview of U.S. and Other Nations’ Laws | Refer to the Required Readings list in the Course Resources folder. | Introductions – Discussion forum (0 – not scored, but required)  
Debate/Discussion Questions in forum  
Four-Page Paper 1 - due week 2 |
| 2          | Continued review of laws and begin review of Regulatory standards | Refer to the Required Readings list. | Debate/Discussion Questions  
No Four-Page Paper this week |
| 3          | Review some international privacy and cyber security law | Refer to the Required Readings list. | Debate/Discussion Questions  
Four-Page Paper 2 - due week 4 |
| 4          | Review of State laws and Cyber Security frameworks/standards | Refer to the Required Readings list. | Debate/Discussion Questions  
Four-Page Paper 3 - due week 5 |
| 5          | What is the definition of “Reasonable Security?” | Refer to the Required Readings list. | Debate/Discussion Questions  
Four-Page Paper 4 - due week 6 |
| 6          | Legal Trends in the Courts | Refer to the Required Readings list. | Debate/Discussion Questions  
Four-Page Paper 5 - due week 7 |
| 7          | Identifying legal issues in cyber and information security | Refer to the Required Readings list. | Debate/Discussion Questions  
Four-Page Paper 6 - due week 8 |
| 8          | Final Project, and Debate/Discussion | Refer to the Required Readings list. | Final Project – Part 1: Four-Page Paper 7 - due week 8  
Final Project – Part 2: Incident Response Scenario - due week 8 |

**Total** | **100%** | (see below for break down per assignment)
Summary of Assignments and Percentage Weight towards course grade

<table>
<thead>
<tr>
<th>Assignments</th>
<th>Weighted Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debate/Discussion Questions (Topics 1-8)</td>
<td>20%</td>
</tr>
<tr>
<td>Four-Page Papers (6)</td>
<td>60%</td>
</tr>
<tr>
<td>Final Project – Part 1: Four-Page Paper</td>
<td>10%</td>
</tr>
<tr>
<td>Final Project – Part 2 – Incident Response Scenario</td>
<td>10%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

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](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](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 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](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.