### Information Security Management
**ITP 370 (3 Units)**

| **Objective** | Upon completing this course, students will:
| - Understand the fundamentals of managing information security systems and personnel
| - Learn how security and management are interrelated
| - Understand the laws and regulations surrounded information security
| - Learn how to plan for disaster recovery
| - Learn how to conduct security audits |

| **Concepts** | This course is designed to teach the fundamentals of security management. The course is not technical in nature, but relies on the student’s previous understanding of security systems. The course instead looks at security from a managerial perspective with regards to design, implementation, maintenance, and disaster recovery. |

| **Prerequisites/Recommended Preparation** | ITP 125 |

| **Instructor** | Joseph Greenfield |
| **Contacting the Instructor** | joseph.greenfield@usc.edu | 213-740-4604 |

| **Office Hours** | TBA |
| **Lecture** | 3 hrs/week |


| **Web Site** | All course material will be on Blackboard at blackboard.usc.edu |

| **Grading** | Grading will be based on assignments, a midterm examination, and a final project. Assignments will be given every week. The grading breakdown is as follows
| Assignments | 50% |
| Midterm | 20% |
| Final Exam | 30% |
| Total | 100% |
## Grading Scale

The following is the grading scale to be used for the final grades at the end of the semester:

<table>
<thead>
<tr>
<th>Percentage Range</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>93% and above</td>
<td>A</td>
</tr>
<tr>
<td>90% - 93%</td>
<td>A-</td>
</tr>
<tr>
<td>87% - 90%</td>
<td>B+</td>
</tr>
<tr>
<td>83% - 87%</td>
<td>B</td>
</tr>
<tr>
<td>80% - 83%</td>
<td>B-</td>
</tr>
<tr>
<td>77% - 80%</td>
<td>C+</td>
</tr>
<tr>
<td>73% - 77%</td>
<td>C</td>
</tr>
<tr>
<td>70% - 73%</td>
<td>C-</td>
</tr>
<tr>
<td>67% - 70%</td>
<td>D+</td>
</tr>
<tr>
<td>63% - 67%</td>
<td>D</td>
</tr>
<tr>
<td>60% - 63%</td>
<td>D-</td>
</tr>
<tr>
<td>Below 60%</td>
<td>F</td>
</tr>
</tbody>
</table>

## Policies

- Projects turned in after the deadline will automatically have 5% deducted per day. Projects will not be accepted after 1 week beyond the project’s deadline.

- No make-up exams (except for medical or family emergencies) will be offered nor will there be any changes made to the Final Exam schedule.

- It is your responsibility to submit your project on or before the due date. **It is not the responsibility of the lab assistant.** Do not turn in anything to your lab assistant!

- All projects will be digitally submitted through blackboard except where specifically specified. Always keep a backup copy of your labs.

## Academic Integrity

The use of unauthorized material, communication with fellow students during an examination, attempting to benefit from the work of another student, and similar behavior that defeats the intent of an examination or other class work is unacceptable to the University. It is often difficult to distinguish between a culpable act and inadvertent behavior resulting from the nervous tension accompanying examinations. When the professor determines that a violation has occurred, appropriate action, as determined by the instructor, will be taken.

Although working together is encouraged, all work claimed as yours must in fact be your own effort. Students who plagiarize the work of other students will receive zero points and possibly be referred to Student Judicial Affairs and Community Standards (SJACS).

All students should read, understand, and abide by the University Student Conduct Code listed in Scampus, and available at: [http://www.usc.edu/student-affairs/SJACS/nonacademicreview.html](http://www.usc.edu/student-affairs/SJACS/nonacademicreview.html)
| Students with Disabilities | Any student requesting academic accommodations based on a disability is required to register with Disability Services and Programs (DSP) each semester. A letter of verification for approved accommodations can be obtained from DSP. Please be sure the letter is delivered to me (or to your TA) as early in the semester as possible. DSP is located in STU 301 and is open 8:30 a.m. – 5:00 p.m., Monday through Friday. The phone number for DSP is (213) 740-0776. |
Course Outline

**Week 1** – Introduction to Security Management
- Role of security
- Organizing security goals
- Relationship between the different players in an organization
**Reading:** Chapter 1

**Week 2** – Legal & Assessments
- Working with the legal department
- Understanding the laws that must be followed
- Internal vs. external audits
- Vulnerability assessments
- Penetration testing
- Risk assessments
**Reading:** Chapters 2 & 3

**Week 3** – Security Policies and Procedures
- Documentation purposes
- Writing good policies
- Writing legally acceptable policies
- Policy review
- Security policy examples
**Reading:** Chapter 4 & Instructor Notes

**Week 4** – Designing the Security Plan
- Designing the security plan
- Solution deployment
- Audit and reporting
**Reading:** Chapter 5 & Appendix A

**Week 5** – Deploying New Projects
- Requirements
- Designing for CIA
- Internal Development vs. 3rd party
- Testing and Piloting
**Reading:** Chapter 6 & Appendix C
**Week 6 – Security Training**
- User awareness
- Management awareness
- Training your security team
- Training methods

**Reading:** Chapter 7

**Week 7 – Monitoring**
- Policy monitoring
- Monitoring the network
- Reviewing audit logs

**Reading:** Chapter 8

**Week 8 – MIDTERM**

**Week 9 – Budgeting and Planning**
- Establishing need
- Building the budget
- Staffing costs
- Hardware/software requirements analysis

**Reading:** Chapter 9 & Appendix B

**Week 10 – Building the security team**
- Working with the previous team
- Security administration
- Identifying new candidates
- Small organizations vs. large organizations

**Reading:** Chapter 10

**Week 11 – Reporting**
- Reporting progress
- Measuring security metrics
- Risk assessment and management
- Evaluating the ROI

**Reading:** Chapter 11

**Week 12 – Incident Response**
- Building an incident response team
- Planning the leadership and roles
- Identifying an incident
- Containing the incident
- Collecting evidence
- Eradication and documentation

**Reading:** Chapter 12 & Instructor Notes
**Week 13** – Developing Contingency Plans
- Physical disasters
- Identifying critical systems and data
- Risk analysis
- Funding & justification
- General procedures
**Reading:** Chapter 13 & Instructor Notes

**Week 14** – Responding to Disasters
- Damage assessment
- Assembling a team
- Response, Resumption, Recovery, and Restoration

**Reading:** Chapter 14

**Week 15** – Conclusion
- Conclusion to the course
- Current jobs in security management

**Week 16** – Final Exam