



**Louisville Metropolitan Campus**  
1031 Zorn Avenue, Suite 200, Louisville, KY  
**Course Syllabus ITM 5600**

<b>Course</b>	ITM 5600 - 58 Information and Communications Security
<b>Instructor</b>	Name: Dr. Norman Auspitz Phone: Home: (502) 244-6133 Cell: (502) 939-7328 Email: auspitzn@yahoo.com
<b>Term &amp; Dates</b>	May 26, 2008 – July 26, 2008 – <b>WEDNESDAY</b> 6-10 PM
<b>Location</b>	Louisville Metropolitan Campus
<b>Course Description</b>	An introduction to the various technical and administrative aspects of information security and assurance. The course provides the foundation for understanding the key issues associated with protecting information assets, determining the levels of protection and response to security incidents, and designing a consistent, reasonable information security system with appropriate intrusion detection and reporting features.
<b>Prerequisites &amp; Incoming Student Competencies</b>	COMP or ITM 5000 – Computer Resources and Information Management or a background in computer operations.
<b>Course Objectives</b>	The purpose of the course is to provide the student with an overview of the field of information security and assurance. Students will be exposed to the spectrum of security activities, methods, and procedures. Coverage will include inspection and protection of information assets, detection of and reaction to threats to information assets, and examination of pre- and post-incident procedures, technical and managerial responses and an overview of the information security planning and staffing functions.
<b>Course Level Learning Outcomes</b>	After completing the course, students should be able to: <ul style="list-style-type: none"><li>• Identify and prioritize information assets.</li><li>• Identify and prioritize threats to information assets.</li><li>• Define an information security strategy and architecture.</li><li>• Plan for and respond to intruders in an information system.</li><li>• Describe legal and public relations implications of security and privacy issues.</li><li>• Present a disaster recovery plan for information assets after an incident.</li></ul>
<b>Materials</b>	Information Security: Principles and Practices, Mark Merkow and Jim Breithaupt, Prentice Hall, Upper Saddle Ridge, N.J. 07458 ISBN 0-13-154729-1 <b>Books at <a href="http://www.mbsdirect.net">www.mbsdirect.net</a>. Credit cards and checks are accepted. Make sure you purchase the correct edition.</b>
<b>Supplemental Resources</b>	Selected documents and/or articles that are relevant to lecture, discussion, or research activities may be provided or assigned throughout the term.

<p><b>Grading</b></p>	<p>Team Project (written report &amp; oral presentation) will account for 40% of final grade. Short position (research) papers will account for 30% of the final grade. Mid-term and final exams will account for 30% of the final grade.</p> <p><b><u>Grades:</u></b></p> <p>A           95-100  A-           90-94  B+           88-89  B            84-87  B-           80-83  C            70-79  F            Less Than 70  I            Incomplete Work</p>
<p><b>Activities</b></p>	<ul style="list-style-type: none"> <li>• Chapter Discussions</li> <li>• Directed readings</li> <li>• 2 - Personal Research Papers</li> <li>• Plan and implement a security project - Team Activity</li> <li>• Midterm and final exams</li> </ul>
<p><b>Policy Statements: University Policies</b></p>	<p><b><u>CONDUCT</u></b></p> <p>Students enrolling in a graduate program at Webster University assume the obligation of conducting themselves in a manner compatible with the University's function as an educational institution. Misconduct for which students are subject to discipline include the following categories:</p> <ol style="list-style-type: none"> <li>1. All forms of dishonesty, cheating, plagiarism, or knowingly furnishing false information to the University.</li> <li>2. Obstruction or disruption of teaching, research, administration, disciplinary procedures, or other University activities, or of authorized activities on University premises.</li> <li>3. Theft or damage to property at the University.</li> </ol> <p>Students who cheat or plagiarize may receive a failing grade for the course in which the cheating or plagiarism took place. Students who engage in any of the above misconducts may be subject to dismissal from the University. To the extent that penalties for misconduct (e.g. theft or destruction of property) are prescribed by law, the University will consider appropriate actions under such laws.</p> <p><b><u>ATTENDANCE POLICY</u></b></p> <p>Students are expected to attend all class sessions of every course. In the case of unavoidable absence, the student must contact the instructor. The student is subject to appropriate academic penalty for incomplete or unacceptable makeup work or for excessive or unexcused absences. Generally, a student who misses more than one four-hour course period (per course) without a documented military or medical excuse and</p>

	<p>advance permission of the instructor should withdraw from the class. The University reserves the right to involuntarily drop enrolled students from classes, which they do not attend. Students who do not attend the first class session, who have not made prior arrangement with the instructor for being absent, will be dropped from the course.</p> <p><b><u>MAKE-UP WORK REQUIREMENTS</u></b></p> <p>For each class missed, makeup work will be assigned and must be submitted at the next class. The instructor will assign the topic and amount of work. This makeup work will be incorporated into the class participation grade. If make-up work is not submitted on time, the student’s final grade will be subject to a reduction of one (1) letter grade.</p> <p>Students are responsible for any class material presented during their absence and any assignments due should be submitted prior to the absence, if possible.</p> <p><b>Drops and Withdrawals</b></p> <p>Should you choose to drop or withdraw from this course, the date on which you notify the university of your decision will determine the amount of tuition refund you receive. Refer to the university policies on drops and withdrawals (published elsewhere) to find out what the deadlines are for dropping a course with a full refund and for withdrawing from a course with a partial refund.</p> <p><b>Special Services</b></p> <p>If you need accommodations for a disability, please let the instructor know at the beginning of the course so that they can be provided.</p> <p><b><u>DISCLAIMER</u></b></p> <p>This syllabus is intended to provide a basic structure to this course. It MAY be modified for class size, student competencies, etc. Adherence to this syllabus is subject to change at the sole discretion of the instructor.</p>
<b>Course Policies</b>	This course will include working on a team project. Team members will have input into the performance appraisal of other team members.
<b>Weekly Schedule</b>	<p>Meeting 1 May 28 – Introduction and course administration Assignment: Chapter 1: Introduction to Information Security</p> <p>Meeting 2 June 04 – Standards and the Security BOK Assignment: Chapter 2: Information Security Principles of Success Chapter 3: Certification Programs</p> <p>Meeting 3 June 11 – Discuss: What are the “BIG” issues in Information Security Assignment: Chapter 4: Security Management Chapter 5: Architecture and Models Prepare &amp; Present: a 3-5 page research paper on the “BIG” Information Security issues.</p>

	<p>Meeting 4 June 18 – Discuss: What does the “ideal security” plan look like? Assignment: Chapter 6: Business Continuity Planning &amp; Disaster Recovery</p> <p>Meeting 5 June 25 – Mid-term – Chapters 1-6 and the research paper findings Assignment: Chapter 7: Law, Investigations, and Ethics</p> <p>Meeting 6 July 02 – Real vs. imaginary physical and operations security Assignment: Chapter 8: Physical Security Chapter 9: Operations Security</p> <p>Meeting 7 July 09 – Access technologies – Research reports on new technologies Assignment: Chapter 10: Access Control Systems Chapter 11: Cryptography Develop : a 3-5 page research paper on new emerging IT security technologies and present during this class.</p> <p>Meeting 8 July 16 – Network Security and Team Paper Presentations Assignment: Chapter 12: Telecommunications, Network &amp; Internet Security</p> <p>Meeting 9 July 23 – Future Systems &amp; Final Exam Assignment: Chapter 13: Application Development Chapter 14: Securing the Future</p>
<p><b>Additional Information</b></p>	<p>Mandatory Topics:</p> <ul style="list-style-type: none"> <li>• Defining the IT Security Plan</li> <li>• Estimating plan times and costs</li> <li>• Scheduling resources</li> <li>• Risk management</li> <li>• Plan execution: measurement, evaluation and control</li> <li>• IT Security tools and techniques</li> <li>• Organizing and leading IT security teams</li> <li>• Issuing recommendations</li> </ul> <p>Course Performance Outcomes:</p> <ul style="list-style-type: none"> <li>• Complete a IT Security Plan with a local organization</li> <li>• Conduct a site and process evaluation</li> <li>• Know IT Security Resources .</li> </ul>