



## **COURSE SYLLABUS**

**Course Name: IA 103**

### **Information Security/Assurance Overview**

#### **Instructor:**

Office Hours:

Office Phone

Office Address:

Email Address:

#### **Course Description**

A study of security in both the voice and data networks and an examination of the security issues associated with the movement toward a convergence of the two infrastructures. Topics to be covered include voice and data network connectivity, modem security, VOIP security, wireless security, cryptography, intrusion detection systems, voice and data firewalls, malicious software, information operations and warfare, and denial of service attacks.

**Purpose:** The purpose of this course is to provide undergraduate level students with an educational experience in the overview of the information assurance field including all aspects of this very broad profession.

**Scope:** The scope of the material to be covered includes:

- Organization goals and leadership roles
- Foundations of security including legal, regulatory and policy issues
- General threats including DNS, spoofing, hijacking, malicious logic.

#### **Course Objectives:**

Upon successful completion of this course, students should be able to:

1. Demonstrate foundation knowledge of information security/assurance within the organization
2. Demonstrate knowledge of the profession, its organizations, goals and leadership roles, literature/publications, issues, and research foundations.
3. Demonstrate knowledge of the foundations of information security including legal, regulatory and policy issues, understanding general threats against information systems

including denial of service, spoofing, and hijacking. Understand how to combat viruses, worms, Trojan horses and logic bombs.

4. Demonstrate knowledge of security objectives and policy development.
5. Demonstrate knowledge of cryptography and public key infrastructure (PKI)
6. Demonstrate knowledge of target hardening of network devices, operating systems and applications.

### **Required Texts and Handouts:**

- Principals of Information Security, Second Edition (2005). Michael E. Whitman and Herbert J. Mattord ISBN-10:0-619-21625-5, ISBN-13: 978-0-619-21625-5.Thomson , Inc.

## **Course Content**

### **Unit 1 Course Expectations and introduction**

- 1.1 Introduction to course, Syllabus Review, Requirements
- 1.2 Introduction and Security Trends

### **Unit 2 Risk management and Policy development**

#### 2.1 Asset Management

- 2.1.1 Background Investigations
- 2.1.2 Delegation of Authority
- 2.1.3 Individuals assigned to perform IA Functions
- 2.1.4 Information Classification, importance of classification
- 2.1.5 General Security Concepts

#### 2.2 Access Control Policy

- 2.2.1 Access Authorization
- 2.2.2 Auditable Events
- 2.2.3 Authentication
- 2.2.4 Biometrics/Biometric Policies
- 2.2.5 Separation of Duties
- 2.2.6 Need-To-Know Controls

#### 2.3 Usage Policy

- 2.3.1 Electronic Records Management, importance
- 2.3.2 Investigative Authorities, importance of
- 2.3.3 Information Marking
- 2.3.4 Non-repudiation
  - 2.3.4.1 Importance and role of non-repudiation
- 2.3.5 Backups
  - 2.3.5.1 Importance of backups
- 2.3.6 Change Control/Configuration Management, Discuss the importance of both

- 2.3.7 Declassification/Downgrade of Media, importance of downgrade of media
- 2.3.8 Business Continuity (BCP/DR)
- 2.3.9 Operational/Organizational Security

## 2.4 Incident Response

- 2.4.1 Countermeasures
- 2.4.2 Destruction/Purging/Sanitization of Classified/Sensitive Information

## 2.5 Awareness Training

- 2.5.1 Education, Training, and Awareness
- 2.5.2 Education, training, and awareness countermeasures implementation

## **Unit 3 Legal, ethical and professional issues in IA**

## **Unit 4 Security Technology**

### 4.1 Access Control

- 4.1.1 Access Authorization
  - 4.1.1.1 Manual/automated access controls
  - 4.1.1.2 Importance of manual/automated access controls
- 4.1.2 Auditable Events
- 4.1.3 Authentication
- 4.1.4 Accountability for Classified/Sensitive Data
  - 4.1.4.1 Classification and declassification of information
    - 4.1.4.1.1 Disposition of classified material
    - 4.1.4.1.2 Remanence
- 4.1.5 Access Privileges
- 4.1.6 Discretionary Access Controls
  - 4.1.6.1 Importance of discretionary access controls
  - 4.1.6.2 Mandatory access controls
- 4.1.7 Biometrics/Biometric Policies
- 4.1.8 Separation of Duties
  - 4.1.8.1 Importance of need to ensure separation of duties where necessary
- 4.1.9 Need-To-Know Controls – Importance of Need to Know Controls

### 4.2 Additional Implementation of Information Assurance

- 4.2.1 Electronic-Mail Security, importance of electronic mail security
- 4.2.2 Public Key Infrastructure
  - 4.2.2.1 Importance and role of PKI
- 4.2.3 Cryptography
- 4.2.4 Automated Security Tools
- 4.2.5 Backups

### 4.3 Risk analysis

- 4.3.1 systems certifiers and accreditors in risk mitigation

## **Unit 5 Physical Security**

## 5.1 Security and Personnel

### **Unit 6 Information Security Maintenance**

### **Unit 9 Physical Security**

#### 9. 1. Facilities planning

##### 9.1.1 Importance of facilities planning

#### 9.4 Interception of data (pg 415)

##### 9.4.1 Discuss connectivity involved with communications

##### 9.4.2 Explain the importance of connectivity involved in communications

##### 9.4.3 Emissions Security (EMSEC) and TEMPEST

###### 9.4.3.1 Discuss threats from Emissions Security (EMSEC)

###### 9.4.3.2 Discuss threats from TEMPEST failures

###### 9.4.3.3 Explain the importance of the threats from Emissions Security (EMSEC)

###### 9.4.3.4 Explain the importance of the threats from TEMPEST failures.

##### 9.4.4 Wireless Technology

###### 9.4.4.1 Discuss threats from electronic emanations

###### 9.4.4.2 Explain the importance of wireless technology

###### 9.4.4.3 Explain the risks associated with portable wireless systems, viz., PDAs

###### 9.4.4.4 Explain the importance of vulnerabilities associated with connected systems wireless technology

### **EMU-Online**

The website [emuonline.edu](http://emuonline.edu) will be used in this course. Class announcements, lecture slides and assignments will be distributed via the e-companion web site. To enroll in EMUonline go to <http://ecompanion.emich.edu>, and then click on "get access" and request access for the course. You are expected to be enrolled online by the second week of class.

Etraining.emich.edu will be utilized for additional readings. Books are accessible thru the Halle library, Books 24x7 web site, <https://ezproxy.emich.edu> and <http://etraining.emich.edu>

### **Grading**

The grades will be made up of the following requirements:

Group project and presentation 25 % (project 20%, presentation 5%)

Individual Project 20%

Two quizzes: 20% (10% ea)

Final exam: 15%

Homework (E-Companion): 20%

Extra credit individual paper: 5%

### **Grading Scale**

Points in each area are cumulated and converted to percent form. The final letter grade is assigned as follows:

|                   |                |                |                |
|-------------------|----------------|----------------|----------------|
| A = 94% and above | B+ = 87 - 89%  | C+ = 77 - 79%  | D+ = 67 to 69% |
| A- = 90 - 93%     | B = 84 - 86%   | C = 74 - 76%   | D = 64 to 66%  |
|                   | B - = 80 - 83% | C - = 70 - 73% | D- = 60 to 63% |
|                   |                |                | E= Below 60%   |

### **Examination policy**

If you do not take an exam at the same time as everyone else in the class, it will be classified as a make-up. It is the responsibility of the student to contact the instructor prior to the next class meeting after missing an exam. The exam should be made-up prior to the next class because it is a general procedure to pass graded exams back to students at that time. If not made-up, a zero will be given for the missed exam.

*Preparing for an exam:* attendance is the key to the getting information in preparation for an exam. At least 90% of the questions are directly from the reading material. Review the chapter summary sections at the end of each chapter and step through the chapter exercises at the end of each chapter.

*Incase you're late or absent:* It's your responsibility to get the course notes, handouts and lab assignments, should you miss class or be late. In nearly every case, lecture presentations will be available on the e-companion site.

### **Dropping class**

To receive a drop (DR) for the class, the student must officially drop the class. A grade for the class will be given according to the materials turned in if the student does not drop the class. Telling the instructor of your intent does not accomplish an official drop. Tuition will be refunded according to the policy stated in the class schedule booklet received during enrollment.

### **Incomplete Policy**

Students will not be given an incomplete grade in the course without sound reason and documented evidence as described in the student handbook, in any case, for a student to receive an incomplete, they must be passing and must have completed a significant portion of the class.

### **Attendance Policy**

Attendance is taken each session. Consistent class attendance is necessary to successfully complete this course. If you will be missing a class, please let me know. Please be punctual and

try to be quiet when leaving or entering the classroom.

### **Classroom Etiquette**

At all times be considerate to your classmates and to your instructor. **No food or beverage is allowed in any classroom.** Come to class on time, ready to ask questions about previous lessons/assignments. Ask pertinent questions; contribute to discussions; avoid "private" conversations that distract the instructor and other students. Please put phones and pagers in silent operational mode.

### **Assignment late policy**

No assignments will be accepted more than two weeks late. Assignments handed in during the week after they are due are penalized 25%. Assignments handed in during the second week after they are due are penalized 50%. Plan to spend approximately six hours weekly on this course. Make sure your name, student ID, and exercise number appear in the assignment.

### **Ethical Behavior**

Students are expected to uphold the school's standard of conduct relating to academic honesty. Students assume full responsibility for the content and integrity of the academic work they submit. The guiding principle of academic integrity shall be that a student's submitted work, examinations, reports, and projects must be that of the student's own work. Students shall be guilty of violating the honor code if they:

1. Represent the work of others, as your own.
2. Use or obtain unauthorized assistance in any academic work.
3. Give unauthorized assistance to other students.
4. Modify, without instructor approval, an examination, paper, record, or report for the purpose of obtaining additional credit.
5. Misrepresent the content of submitted work.

### **Plagiarism**

The Internet is a valuable tool, but not a replacement for your own thoughts. For all papers and assignments in this class, Do NOT cut and paste from the internet, you must formulate your own ideas based on the literature. Anything you use directly should be quoted with citation noted.

Please read this web page: <http://owl.english.purdue.edu/owl/> , you may or may not know this but it will give you guidelines. If you're in doubt, ask me! All submitted papers can follow either MLA or APA guidelines.

Couple of links, there is a large volume of material contained within the two websites. Keep them for your future reference.

- Plagiarism Guidance: <http://www.emich.edu/halle/plagiarism.html>
- Citation and reference help: [http://www.emich.edu/halle/style\\_guides.html](http://www.emich.edu/halle/style_guides.html)

**Disabilities Policy**

In compliance with the Americans with Disabilities Act (ADA), all qualified students enrolled in this course are entitled to "reasonable accommodations." Please notify the instructor during the first week of class of any accommodations needed for the course.

## Tentative Schedule

| <b>Date</b> | <b>Week</b> | <b>Topic</b>                                    | <b>Chapter</b> | <b>Additional</b>           |
|-------------|-------------|---|----------------|-----------------------------|
| 1/8         | 1           | Course Expectations and introduction            | 1              |                             |
| 1/15        | 2           | Need for Security                               | 2              | <b>Assign paper 1</b>       |
| 1/22        | 3           | Legal, ethical and professional issues in IS    | 3              |                             |
| 1/29        | 4           | Risk Management                                 | 4              |                             |
| 1/31        | 4           | <b>Quiz 1 (Chapters 1 – 3)</b>                  |                |                             |
| 2/5         | 5           | Planning for Security                           | 5              |                             |
| 2/12        | 6           | Security Technology                             | 6              |                             |
| 2/19        | 7           | Security Technology                             | 7              | <b>Paper 1 due</b>          |
| 3/4         | 8           | Cryptography                                    | 8              | <b>Assign group project</b> |
| 3/11        | 9           | Physical Security                               | 9              |                             |
| 3/13        | 9           | <b>Quiz 2 (Chapters 4 – 8)</b>                  |                |                             |
| 3/18        | 10          | Implementing Information Security               | 10             |                             |
| 3/25        | 11          | Business Continuity (BCP/DR)                    |                |                             |
| 4/1         | 12          | Security and Personnel                          | 11             |                             |
| 4/8         | 13          | Information Security Maintenance                | 12             |                             |
| 4/15        | 14          | <b>Group Presentations</b>                      |                |                             |
| 4/24        | 15          | <b>Final Exam(1 – 2:30) Chapters 9 – 12 and</b> |                |                             |