New York University Tandon School of Engineering
Computer Science & Engineering
Course Outline CS-GY 6803
Information System Security and Management

Spring 2020
Professor Mike Wilkes
Online Course

To contact professor: mwilkes@nyu.edu
Phone: **(929) 267-3137**

Course Pre-requisites: Graduate status and CS-UY 3923 or equivalent

Course Student Survey: https://nyu.qualtrics.com/jfe/form/SV_b2Aol24Y23VvurH

Course Description
This course presents a system and management view of information security: what it is, what drives the requirements for information security, how to integrate it into the systems-design process and the life-cycle of information systems. A second goal is to cover basic governance, risk and compliance with regard to information security policy management as required by GDPR, CCPA, and NYDFS. Topics include information security risk management, security policies, security in the systems-engineering process, laws related to information security and the management of operational systems.

Course Zoom Link: https://nyu.zoom.us/my/mwilkes

Course Objectives
This course will have achieved it's objectives if afterwards you:

1. understand and discuss core concepts and principles of information security
2. appreciate the importance of data classification with regard to risk management
3. are able to describe and understand the phases of incident response
4. become familiar with the practice of information systems security engineering
5. understand the role of compliance and audit with regard to design, documentation, testing, monitoring, business continuity planning and automation

Course Structure
Weekly Lecture Hours: 2.5 | Weekly Lab Hours: 0 | Weekly Recitation Hours: 0

Readings
While there is no single textbook which covers most of the material in this course in a complete or exhaustive manner, two books have been used in the past as valuable references:

Whitman and Mattford, *Management of Information Security*, Sixth Edition,
ISBN-13: 978-1337405713, ISBN-10: 133740571X, Cengage Learning, 2019.

- This text provides a good general reference for risk analysis, policy, standard security management processes.

Anderson, *Security Engineering*, Second Edition,
ISBN-13: 978-0470068526, ISBN-10: 0470068523, Wiley, 2008.

- An excellent book on many aspects of security
- More oriented towards technology than management
- Great examples of the results of good security engineering in the real world, including system flaws
- Reflects a system view of security, but does not reflect a systems engineering process view or how to get there.

Other references: various web sites, articles, books and research papers are listed as reading assignments on a per lecture basis.

Grade Calculation

The course grade is based on a project (40%), homework (40%) and participation (20%). Your participation is comprised of Tandon School of Engineering Discussion Forum participation as well as your correspondence with the instructor and your classmates. There is no mid-term or final examination.

Course requirements

As this is an online course, a new lecture is delivered each week. Homework assignments and mandatory discussion topics are posted at the same time. A team project is also required.

The team project is comprised of teams of 3-4 students. Students form their own teams and select a project within the guidelines presented. Team projects must be approved by the instructor. If required, teams will be adjusted to ensure a balanced mixture of learning styles and profiles.

Once the project teams are formed, send an email describing the proposed project by the end of week 2. Final approved project proposals are due by week 3.

A Team Project Proposal consists of:

- Team Name (one of the hardest things we do in IT is to name things):
- Project Objective:
- Mission Statement:
- Project Plan:
- High Level Diagram:
- Project Outcomes:

Team Project Deliverables:

- Draft Project Proposal by week 2 (PDF)
- Final Project Proposal by week 3 (PDF)
- Draft Project Report by week 6 (PDF)
- Draft Project Executive Presentation by week 9 (slides)
- Final Project Report due on semester final exam date (PDF, slides & video recording of Executive Presentation)

Homework and Reading Assignments
You have 8 days following the posting of the homework, reading assignments and discussion topics to submit your work. Observed holidays will be taken into account with additional time provided. You are responsible for the materials in the reading assignments.

Discussion Forum
Each live Zoom lecture will have an accompanying discussion with one or more posts. Participation is mandatory in the discussions each week.

Reading Assignments
The core reading assignments are identified as such. Supplemental readings will be listed separately and are optional, but are useful and relevant examples from the real world that reinforce the topics and themes of the lecture and homework for that week.

The practice of Information System Security is at the core of this course. All aspects of managing information security tools, processes and teams cannot be covered in one semester. But the essentials of praxis (theory and practice *combined*) can and will be exercised over the course of this 14 week class. Your participation level, however, will to some degree determine just what you get out of the class. I can enthuse at you for 35 hours (14 Saturday lectures of 2.5 hours each), but at the end of the day the degree to which you will be inspired and engaged is in your own hands.

Part I: Introduction

[2/1] Week 1: Information Security and Risk Management
- Course Introduction
- What is Information Security? What is Risk?

[2/8] Week 2: Information Systems Security Technique
- People, Process and Tools
- Identity & Access Management
- Privileged Identity Management

[2/15] Week 3: Data Classification
- Data-centric Security vs Perimeter-based Security
- Types of Data: Structured and Unstructured
- Data and the future of Privacy Engineering

[2/22] Week 4: Information Systems Engineering
- Legacy Designs
- Modern Reference Architectures
- Configuration Management/Drift
- Asset Management

Part II: Managing Information Systems Security

[2/29] Week 5: Incident Response
- Phases of Incident Response
- NIST Cyber Security Framework
- ITIL v4 (former acronym: Information Technology Infrastructure Library)

[3/6] Draft Team Project Report Due

[3/7] Week 6: Vulnerability Management
- OS Security Patching
- Application Patching
- Vulnerability Scanning

[3/14] Week 7: Business Continuity Planning
- Business Impact Analysis
- Disaster Scenarios
- BCP/DR Testing

[3/16] Spring Recess

[3/28] Week 8: Documentation and Design
- Diagrams: High Level, System, Data Flow
- Runbooks, Wikis, Release Notes and Repositories
- Threat Modeling

[4/3] Draft Project Executive Presentation Due

[4/4] Week 9: Testing and Automation
- Application Testing
- Penetration Testing
- Scripting, Infrastructure as Code and DevSecOps

[4/11] Week 10: Governance, Risk and Compliance
- The Executive Management Perspective
- "Reasonable" Security Controls and Lawyers
- Compliance and Regulatory Requirements

(GDPR, PCI, SOX, HIPPA, CCPA, NYPA, etc)

[4/18] Week 11: Audit and Observability
- Change Control and SDLC
- Who's Watching the Watchers?

[4/25] Week 12: Information Security Policy
- WISP: Written Information Security Policy
- SIRP: Security Incident Response Policy
- Social Media Policy

[5/2] Week 13: Monitoring and Threat Intelligence
- Alerts, Tickets and Logging
- Basic, Functional, Performance and Security Monitoring
- Keeping abreast of Trends and News

[5/9] Week 14: Training and Security Awareness
- Phishing Awareness Testing
- Secure Development Best Practices
- Tabletop Exercises and Red Team Exercises

[May 15, 2020] [Final Project Report Deliverables Due]

Moses Center Statement of Disability
If you are student with a disability who is requesting accommodations, please contact New York University's Moses Center for Students with Disabilities (CSD) at 212-998-4980 or mosescsd@nyu.edu. You must be registered with CSD to receive accommodations. Information about the Moses Center can be found at www.nyu.edu/csd. The Moses Center is located at 726 Broadway on the 3rd floor.

NYU School of Engineering Policies and Procedures on Academic Misconduct – complete Student Code of Conduct here

A. Introduction: The School of Engineering encourages academic excellence in an environment that promotes honesty, integrity, and fairness, and students at the School of Engineering are expected to exhibit those qualities in their academic work. It is through the process of submitting their own work and receiving honest feedback on that work that students may progress academically. Any act of academic dishonesty is seen as an attack upon the School and will not be tolerated. Furthermore, those who breach the School's rules on academic integrity will be sanctioned under this Policy. Students are responsible for familiarizing themselves with the School's Policy on Academic Misconduct.

B. Definition: Academic dishonesty may include misrepresentation, deception, dishonesty, or any act of falsification committed by a student to influence a grade or other academic evaluation. Academic dishonesty also includes intentionally damaging the academic work of others or assisting other students in acts of dishonesty. Common examples of academically dishonest behavior include, but are not limited to, the following:

1. Cheating: intentionally using or attempting to use unauthorized notes, books, electronic media, or electronic communications in an exam; talking with fellow students or looking at another person's work during an exam; submitting work prepared in advance for an in-class examination; having someone take an exam for you or taking an exam for someone else; violating other rules governing the administration of examinations.
2. Fabrication: including but not limited to, falsifying experimental data and/or citations.
3. Plagiarism: intentionally or knowingly representing the words or ideas of another as one's own in any academic exercise; failure to attribute direct quotations, paraphrases, or borrowed facts or information.
4. Unauthorized collaboration: working together on work meant to be done individually.

5. Duplicating work: presenting for grading the same work for more than one project or in more than one class, unless express and prior permission has been received from the course instructor(s) or research adviser involved.
6. Forgery: altering any academic document, including, but not limited to, academic records, admissions materials, or medical excuses.

NYU School of Engineering Policies and Procedures on Excused Absences – complete policy here

A. Introduction: An absence can be excused if you have missed no more than **10 days of school.** If an illness or special circumstance has caused you to miss more than two weeks of school, please refer to the section labeled Medical Leave of Absence.

B. Students may request special accommodations for an absence to be excused in the following cases:

1. Medical reasons
2. Death in immediate family
3. Personal qualified emergencies (documentation must be provided)
4. Religious Expression or Practice

Deanna Rayment, deanna.rayment@nyu.edu, is the Coordinator of Student Advocacy, Compliance and Student Affairs and handles excused absences. She is located in 5 MTC, LC240C and can assist you should it become necessary.

NYU School of Engineering Academic Calendar – complete list here.
Please pay attention to notable dates such as Add/Drop, Withdrawal, etc.

For confirmation of dates or further information, please contact Susana: sgarcia@nyu.edu