Course Outline 2015
INFOSYS 341: MANAGEMENT OF INFORMATION SECURITY
(15 POINTS)

Semester 1
_____

Course Prescription

An overview of activities, methods, methodologies, and procedures related to establishing sound information security policies. Topics include: defining security requirements; security management models and practices; risk management; identification and authentication; access control; information security technologies and encryption techniques. Some key legal and ethical issues associated with the management of information security will be discussed.

Programme and Course Advice:

Prerequisite: 15 points from INFOSYS 220 or INFOSYS 222 or INFOSYS 223 or INFOSYS 224 or ACCTG 222 or INFOMGMT 291,292.

Goals of the Course

The purpose of the course is to provide the student with an overview of the field of Information Security from a management perspective. Students will be exposed to the spectrum of security activities, methods, methodologies, and procedures. Coverage will include inspection and protection of information assets, the management of risk, the detection of and reaction to threats to information assets, and an overview of the Information Security Planning and staffing functions.

Lab will introduce students to the basic technical concepts related to information security.

Learning Outcomes

By the end of this course it is expected that a student will be able to:

1. identify and prioritize information assets;
2. identify and prioritize threats to information assets;
3. define an information security strategy and architecture;
4. define information security policy and understand its central role in a successful information security program
5. define risk management and its role in the organisation;
6. describe the various access control approaches including authentication, authorisation, and biometric access controls;
7. plan for and respond to intruders in an information system;
8. identify the skills and requirements for information security positions;
9. describe legal and public relations implications of security and privacy issues;
10. present a disaster recovery plan for recovery of information assets after an incident; and
11. apply project management principles to an information security program.

Content Outline

Lectures (Subject of possible changes)

Session	Topic
1	Introduction to information security, The need for security
2	Security profession, Pen testing, Cryptography
3	Computer Forensic, Cryptography
4	Legal, ethical and professional issues in information security
5	Risk Management: identifying and assessing risk
6	Planning for security
7	Firewalls and VPNs
8	Intrusion Detection, Access Control
9	Physical security
10	Implementing Information Security
11	Security and Personnel
12	Information security maintenance, course summary

Security Lab topics (starting at the third week of the term, subject of possible changes)
1. Cryptography I
2. Cryptography II
3. Steganography
4. Computer forensic
5. Firewalls
6. Linux Security essentials
7. WEB Goat I
8. WEB Goat II
9. Lab assessment test

Learning and Teaching
- The course will be delivered at the City Campus 3 hours per week during 12 weeks.
- Active audience is expected during lectures.
- Lectures will be recorded
- Special file called INDEX will be visible on Cecil. You will find there information whcich topic had been covered in the class presentation, corresponding slides and other study materials plus important class announcements.

Learning Resources
- M. Whitman and H. Mattord. Principles of Information Security, Thomson - Course Technology, 2015, Fifth Edition
- Software used in lab: Provided by Instructor
- Lectures notes distributed via Cecil
- Links to related publications in newspapers, magazines and journals will be provided from time to time

Teaching Staff

A/P Lech Janczewski, Email: lech@auckland.ac.nz, Phone: 923 7538, Office: room OGGB 480

Tutors
Andrea Herrera, Email: a.herrera@auckland.ac.nz
Khairulliza Salleh, Email: k.salleh@auckland.ac.nz
Farzan Kolini, Email: f.kolini@auckland.ac.nz

Assessment

Group project: research essay	20%
Lab: exercises	8%
Lab: test	12%
Mid semester Test (WED, 9.04)	20%
Final Exam	40%
	____
Total	100%

To complete this course you must score at least 30 points (total) from Mid term Test and Final examination (combined). Failing to do so will result in the D grade irrespective of the coursework results.

Further details on these assessments will be provided at the first lecture.

The broad relationship between these assessments and the course learning outcomes is as follows:

Learning Outcome	Lab	Group Project	Test	Exam
1			X	X
2	X	X	X	X
3		X	X	X
4		X	X	X
5		X	X	X
6	X	X		X
7			X	X
8	X	X	X	X
9		X		X
10		X		X
11	X	X		

Inclusive Learning
Students are urged to discuss privately any impairment-related requirements face-to-face and/or in written form with the course convenor/lecturer and/or tutor.

Student feedback
- Students will be asked to provide twice the semester evaluation of the course.

Course regulations

- This is a paperless course: All students' assignments and returned submissions will be done electronically, mostly via Turnitin system. Detailed instruction will be provided latter.
- All course materials (like PP slides, readings, assignments, etc.) will be available via Cecil. Class notes will be placed on Cecil two days before presentation.
- All other important class information will also be distributed via Cecil.
- Office hours are Mondays, 13:00-15:00.
- You may send a query via email, but limit it to issues which would require a short reply (no more than a sentence). Longer queries: office hours only. Any electronic query will be answered the next working day (if not sent after 16:00). This means that do not expect a Friday night query to be answered before Monday morning.
- The delivery time of the group project and reports is 1600h. After 1600h Turnitin system will be closed and you should send the submission directly to the supervisor of given activity.
- Late submissions policy:
  - Every started day (after 1600h deadline) will substrates 0.5p from your final course grade,
  - Only substantial health or personal problems would qualify for a possible extension of a submission date. But 1 day before the deadline the submission date would not be a subject of any negotiations.
- Cecil will be used for sending the important messages, including possible **request for answer.**
- "Request for answer" messages
  - Some messages might be distributed (electronically) from time to time bearing letters RA (Request for Answer) in the header.
  - You are responsible for reading and acting upon all these messages within the time constrains indicated in the message.
  - Lack of action if it is a RA will result in a deducting 1p penalty per every started day of delay (1600h deadline applies).
- Students are advised that they may not copy or distribute any portion of the materials delivered to them via this course to any third party.
  - A related declaration is provided on Cecil. You need to download it, sign and return during TUE 17 March class. **This is the RA activity.**