Information security – Standards and Best Practices

1. **Course number and name:** 020ISSES5 Information security – Standards and Best Practices

2. **Credits and contact hours:** 4 ECTS credits, 2x1:15 contact hours

3. **Instructor's or course coordinator's name:** Jean-Michel Kaoukabani

4. **Text book:**
   a. **Other supplemental materials:**
      Slides in PowerPoint, articles, videos, and handouts.

   References:
   ISO 27002-2013
   PCI DSS V 3.2
   NIST SP 800-30 Guide for Conducting Risk Assessments
   NIST SP - 800-88 Guideline for media sanitization
   NIST SP 800-53 Recommended Security Controls for Federal Information
   NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View
   http://www.nist.gov/manuscript-publication-search.cfm?pub_id=150444 - (A Unified Framework for Mobile Device Security)

5. **Specific course information**
   a. **Catalog description:**
      An introductory session on key concepts and risk analysis is delivered before discussing the various IT security standards, best practices, standards and guidelines. This course will discuss the ISO 27001-2 2013 standard, PCI DSS, OWASP, SANS-CIS top 20 cyber security controls. This course covers the following areas: Security policy and procedures, human resources security, physical and logical security of systems and networks, incident management and business continuity management.

   b. **Prerequisites or co-requisites:**

   c. **Required:** Elective for CCE students

6. **Specific goals for the course:**
   a. **Specific outcomes of instruction:**
      - Understand the difference between data and information, the definition of an Information System.
      - Understand key concepts (risk, control and vulnerability), risk measurement techniques and selection of appropriate controls.
      - Configure and manage a security policy.

- Understand the techniques for managing and organizing IT security within a company.
- Identify information and data in a professional environment, define ownership and establish classification procedures to ensure appropriate protection and optimal distribution of controls.
- Develop the controls and procedures required to ensure the security of human resources in accordance with international standards and guidelines.
- Understand the requirements of international physical security standards and recommend the necessary controls for physical and environmental security in a data center. Students must be able to set up physical and environmental safety checklists.
- Implement procedures that govern secure information exchange, capacity planning, Internet security, media security, data security, e-commerce security, monitoring and reporting controls and incident handling.
- Define the security requirements of an Internet Banking and Mobile Banking project.
- Define the logical access security requirements of an operating system or application and set up security checklists.
- Procedures for classifying and managing incidents.
- Familiarize students with the business continuity development cycle and the content of a continuity plan.

7. KPI addressed by the course:

KPI	a2	c1	c2	f1	g1	g2	j1
Covered	x	x	x	x			x
Assessed	x	x	x	x	x	x	x
Give Feedback							

8. Topics and approximate lecture hours:

Session number/duration	Description
1 2h 30’	Introduction to Information systems Key concepts in Information Security The Need for Information Security How to define security needs
2 2h 30’	The starting point for information security Risk assessment methods and techniques Selection of controls
3 2h 30’	Security policy
4 2h 30’	Organization of information security and asset Management

Session number/duration	Description
5 2h 30’	Human resources and Information Security
6 2h 30’	Physical and Environmental Security Communication and Operations management
7 2h 30’	Access Control
8 2h 30’	Incident Handling and Business continuity management
9 2h 30’	PCI DSS Standard -12 Requirements
10 2h 30’	OWASP top 10 Vulnerabilities
11 2h 30’	ISO 27002
12 2h 30’	SANS and CIS top 20 Cyber security Controls
13 &14 2x2h 30’	Guided exercises