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. **Name(s) of instructor(s) or course coordinator(s):** Jean-Michel Kaoukabani

4. **Instructional materials:** Slides in PowerPoint, articles, videos, and handouts.

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 2022 standard, PCI DSS 4.0, OWASP, SANS-CIS V8 top 18 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:** None

   c. **Selected Elective**

6. **Educational objectives 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.

b. PI addressed by the course:

PI	2.1	2.4	2.5	3.1	3.2	4.1	5.1	7.1
Covered	x	x	x	x	x	x	x	x
Assessed	x	x	x	x	x	x	x	x

7. Brief list of topics to be covered

- Introduction to Information systems, Key concepts in Information Security, The Need for Information Security, How to define security needs (2 lectures)
- The starting point for information security, Risk assessment methods and techniques, Selection of controls (2 lectures)
- Security policy (2 lectures)
- Organization of information security and asset Management (2 lectures)
- Human resources and Information Security (2 lectures)
- Physical and Environmental Security, Communication and Operations management (2 lectures)
- Access Control (2 lectures)
- Incident Handling and Business continuity management (2 lectures)
- PCI DSS Standard -12 Requirements (2 lectures)
- OWASP top 10 Vulnerabilities (2 lectures)
- ISO 27002 (2 lectures)
- SANS and CIS top 18 Cyber security Controls (2 lectures)
- Guided exercises (2 lectures)