Group members: Ijiehon, Ehis // Hussain, Areeb // Aboualnaga, Khaled

---

## Task #1: Describe what an ISMS is about and formulate a general policy following ISO 27k2

In the context of Information Security, information stands for all the digital and non-digital data and assets. Information security is responsible for implementing, maintaining and improving the information security management systems to keep this information secure, well-maintain in a complete form. **ISMS** provide a secure processing of business to ensure improvement and continuity without interruption by malicious parties from internal and external sources. For departments such as finance, data confidentiality and integrity should be ensured. Task of the Information Security Management are:

### Goals of ISMS for University

- Privacy and protection of personal information of students and staff.
- Prevent physical access of unauthorized personnel from accessing sensitive locations (database)
- Ensuring backup of grades and Examination material in case of a system failure or an unprecedented accident (Fire, blackout)

### Main Components of ISMS

**1) Names/Roles**

**a) Chief Information Security:** Head of Information Security. Responsible of controlling, documentation and reporting to top management.
**b) Information Security Officer:** ISO is responsible of actions to take care of the risk according to ISMS policy and shall report to the information security management. They also do risk analysis.
**c) IT Administrator:** IT Administrator is responsible of personal are obeying security policies.

**2) How to Identify and assess risk**
**a) (C: Confidentiality | I: Integrity | A: Availability)**

**University:** The university helps in providing with new knowledge and skills needed to meet the challenges of sustainable development in a community. The most important role they have been assigned is the production of highly skilled manpower and research output to meet perceived targets, students and management staff's data are available to the university such as address, date of birth, grades and other scientific and software materials. Grades are rewarded to student's on performance. Therefore, there should be integrity and all data should be secured. **C +++ | I ++++ | A ++**

**b) Risk treatment:** Risk Treatment is the process of selecting and implementing of measures to modify risk. Key takeaway of risk treatment is (Avoidance, Retention, Sharing, Transferring, Loss prevention and reduction). It is also important to keep on improving the ISMS; therefore, the PDCA cycle of continuous improvement processes is often implemented. The PDCA cycle consists of 4 different processes:
**Plan:** Identify risks and risk reducing measurement
**Do:** implement risk reducing measurements
**Check:** Verify that measurements in fact reduces the identified risks
**Act:** Review/Extend risk reducing measurements
And repeat

**3) How to organize the documentation**

The organization's information security management system shall include:

- Documented information determined by the organization as being necessary for the effectiveness of the ISMS.

- The size of organization and it's type of activities, processes, products and services.

- There are many techniques to handle threats for i.e. security documentation hierarchy which is establishing a pyramid like hierarchy that illustrates how certain documents are important like passwords policies etc.

**4) How to improve ISMS**

**a) CIP:** CIP security is a method of securely transmitting data at the protocol level, rather than relying solely on additional hardware or applications to provide protection.

- Security authentication: CIP security prevents another device on the network from masquerading as another device
- Data integrity: CIP security identifies if data has been changed in any way
- Encryption: It can encrypt data between various endpoints to protect the data.

**First describe in a few sentences whether the University's business targets are dependent on the security to the Information systems – internal and external systems.**

The university has personal data of students and managements staff; therefore, this makes the university highly dependent on Information Security System (Internal or External) because for i.e. in case of External threat like malware and DDoS attacks or Internal threats like Electrical failures and Hardware errors or sabotage. Such threats expose and manipulate such sensitive data, and this is against the European General Data Protection Regulation.

**General Information policy**

**--** In reference to IS0 27002, 5.1.1:

*Low-level policy should include:*

- **Access control (9):** Users should only be provided with access to the network services that they have been specifically authorized to use; Such as student should have access to certain data like been able to view grades but not allowed to make changes to the grade.
- **Backup, (clause 12.3):** To protect against loss of data, backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy. There should be back up system for university data to avoid permanent loss of data such as student's grade.
- **Privacy and protection of personal identifiable information (18.1.4):** Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable.

*High-level policy should include:*

- **Physical and environmental security (11):** Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
- **Clear desk and clear screen (11.2.9):** A clear desk policy for papers and removeable storage media and a clear screen policy for information processing facilities should be adopted. Unauthorised use of electronic device such as printer and computer should be prevented.
- **Information transfer (13.2.1):** Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities; There should be a sense of security with regards to using the university email such information should be protected from interception, copy, modification, mis-routing and destruction.
- **Protection from malware (12.2):** Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness; When an unrequested software is installed on an individual's computer and/or on an IHE's server, thereby restricting access and/or causing a system crash, it can be considered malware.