ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

Assignment Week 1 – ISO 27001

Master – Cyber Security and Resilience

Group 4 - St. Pölten University of Applied Sciences

Flita-Vasile Adrian – cr221504

Adithyan Shyni Manoj – cr221506

Rakesh Vijayan – cr221515

Alen Marian Varkey Vanisseril– cr221509

Course: Information Security Management

Lecturers: Peter Schoenegger, Simon Tjoa

Semester: WS 2022

St. Pölten, 19.10.2022

Topic: Exercise Organization

The St. Pölten University of Applied Sciences, or Fachhochschule St. Pölten in German, offers higher education in the fields of social sciences, digital business & innovation, health sciences, rail technology & mobility, and computer science & security. Interdisciplinary scientific discoveries, products, and solutions for business and society are made possible by the interdisciplinary mixing of subject areas in teaching and research. Currently, 3.700 students are enrolled in various study programs and continuing education courses to receive a practice-oriented academic education.

The St. Pölten University is a part of the **Education Industry** whose primary objective is to provide education. This establishment is privately owned and operated for profit.

The services that St. Pölten University is offering at the moment are:

- Services for Management and Organisation
- Academic Services that consist of numerous Bachelor and Master programmes and also Continuing education (part time) programmes which numerous fields of study.
- Services for Research and Knowledge Transfer. At the moment there is a number of 112 Research Projects: 30 Contract research projects, 82 Financed by third-party funds, 47 With coordination tasks (out of 82 projects financed by third-party funds).

The total **number of employees** is: 5289 people. There are 138 full-time teaching and academic staff members and 989 part-time teaching-staff, 393 full time staff, 81 academic staff, and 3.688 students.

Turnover:

The total revenues of the Fachhochschule St. Pölten GmbH including the wholly owned subsidiary Fachhochschule St. Pölten ForschungsGmbH amounted to 36.1 million EUR. These total revenues are divided:

1. 28.411 MILLION EUR revenues from teaching
2. 1.791 MILLION EUR other revenues
3. 1.789 MILLION EUR revenues from further education
4. 4.131 MILLION EUR revenues from research, development, innovation, knowledge transfer (incl. ForschungsGmbH)

Locations:

- Campus St. Pölten: Buildings A, B, C Campus-Platz 1, A-3100 St. Pölten
- Location D Heinrich Schneidmadl-Straße 15, 3100 St. Pölten

Customer structure:

The customers that benefit from the university services are:

Students that are attending to Bachelor and Master programmes.
Contractors that apply for the Research programmes and also the third parties that are financing them.
Clients that are benefiting for the event organization.

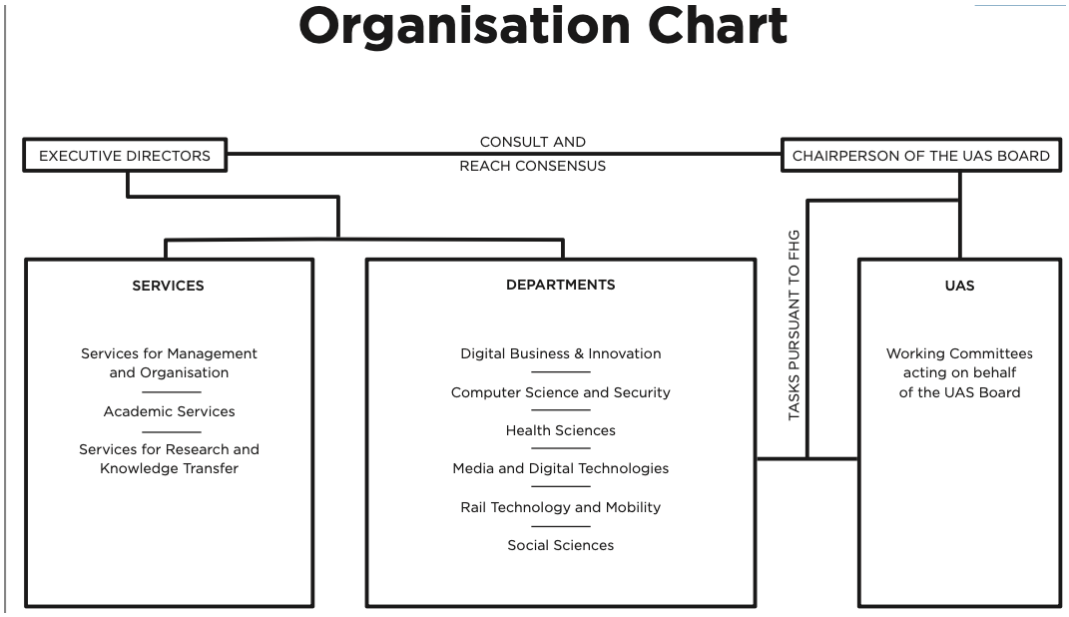
Structure of the organization.

On top of the pyramid are placed the **EXEVUTIVE DIRECTORS** who are seeking consult and reach consensus to **CHAIRPERSON OF THE UAS BOARD.**

These two are followed by the Academic departments is formed of:

- Digital Business & Innovation
- Computer Science and Security
- Health Sciences
- Media and Digital Technologies
- Rail Technology and Mobility
- Social Sciences

And the **UAS** that are working Committees acting on behalf of the UAS Board.



Topic: Stakeholder

The 74% of University of St Polten is privately held, whose sole shareholder is the State Capital St. Polten. And the remaining 26% held by the province of Lower Austria. The provincial government, as the highest administrative body, implements the regional laws, manages the province's finances and administers the province's assets. It is supported by the Office of the Lower Austrian Government. The State Capital St. Polten is a ruling body. So the backbone of this university is both the governing bodies. They are generating revenue of about 36.1 million EUR from conducting this University.

Stakeholder	Internal/External	Information Security needs	Impact and Personal Goals
Executive Bodies and Officers	Internal	24*7 Uninterrupted business process	High impact, Achieve maximum business output
HR Department	Internal	Employee data confidentiality, Other business data confidentiality	Medium impact, Helps in business process
Finance Department	Internal	Ensure security of confidential payment details and other financial records.	Medium Impact, Helps in business process and cash flow management
Marketing Department	Internal	Confidentiality of marketing strategies so that other competitors cannot find out organizations' next move.	Medium Impact, Focused on business expansion process
Academic department & Heads	Internal	Students data controls and access	High Impact, Focused on academic improvement.
Employees - 367	Internal	> Sensitive personal information. > Employee Payment details.	Medium Impact, Working on different departments to achieve organizational goals.
Students	External	Large amount of personal data Payment details.	High Impact, students are the major customers of the organization.

Competitors	External	The statistical and improvement strategies should be hidden.	Low Impact,
Service Providers	External	Data protection should be ensured while dealing with the external Internet service providers. • Seamless power supply is necessary for uninterrupted working.	Medium Impact, Provide necessary services for the organization.
Government	External	Shareholders of the organization are State Capital St Polten and Province of Lower Austria.	High Impact, Promoting Organization growth.

Topic: Goal setting / target setting

Organization's Objective

- **Providing the best education**
- **Providing the best IT and Infrastructure**
- **Providing the best Campus Facilities**
- **Building international relations**

1) How does information security relate to the organization's objectives?

Organizations need to be confident that they have strong data security and that they can protect against Cyber Attacks and other unauthorized access and data breaches. Weak data security can lead to key information being lost or stolen, creating a poor experience for the students and the employees that can lead to loss of Value and reputational harm.if an organization does not implement sufficient protections over user data and information security, weaknesses are exploited by hackers.
For our University it's very essential to have proper information security. If any information security flaws occur, it can seriously harm the future of the students who are studying at the university. The information security provides the CIA features which are essential for the university objectives.

2) In order to achieve their objectives, which requirements does information security have to meet?

In Accordance to meet these objectives proper and advance information security measures should be taken, Including

Confidentiality: controlling who gets to read information;

Integrity: assuring that information and programs are changed only in a specified and authorized manner;

Availability: assuring that authorized users have continued access to information and resources.

In University, Student/Teacher or any employee is giving most of the information regarding studies and personal information Including the bank details which the fee/Salary has been paid, Also the payments details with the partner Universities so It's the responsibility of the organization to keep this data, information secure/Confidential.

In an organization there will be a website/multiple websites for various purposes. The information that's stored in the database should be Well organized and integrated. If it is not properly integrated information leakage will occur.

For example, in the database information about all the students are stored if it is not properly integrated then if a student can view another student's confidential information it is considered as a serious issue, so integrity is a major factor here.

Also the third factor Availability The information regarding every event happening at the university should be available for the users. Also downloading certain documents from the portal etc. should be always available to the users.

3) What risks would exist if the achievement of objectives were not included?
If these objectives are not met then there will be severe consequences, if proper/advance information security is not implemented in the organizations both the users(students/employees) also the university itself should face several problems such as;

- Increase of Theft and Vandalism
- No Procedure to Handle Incidents
- Employees/Students Feeling Unsafe
- Tarnished Business Reputation
- Legal Liability

4) How can one measure or evaluate whether information security supports this goal in an effective manner?

* Audit processes
* Vulnerability assessment and Penetration Testing
* Information security risk management process

*Information security risk assessment
*ISO 27001 certification

By evaluating these factors we can measure how well The ISMS supports the goal in an effective manner. Also the IT department should do constant monitoring and security checkups.

* Having an effective ISMS can provide many benefits to the organization. This is especially true in today's threat-heavy landscape where having robust information security is an absolute necessity in many sectors.

- Help you win new Achievements and enter new sectors
- Strengthen your relationship with your existing students/employees
- Build your organization's Name and reputation
- Protect your Organization from security breaches
- Safeguard your organization's information assets
- Make it easy to demonstrate how secure your information is
- Show how seriously your organization takes information security
- Help you stay ahead of new Information security risks and opportunities
- Support your organization's development and growth

A Strong IT department and Solid infosec reduces the risks of attacks in information technology systems, applies security controls to prevent unauthorized access to sensitive data, prevents disruption of services via Cyber Attacks like denial-of-service (DoS attacks), and much more.

Topic: Scope and boundaries of a management system for information security

Boundaries:
Boundaries of an organization is classified into 3 categories;

Organizational Boundaries:
Organizational boundaries are socially constructed distinctions created intentionally to foster specific patterns of behavior by one set of individuals that are different from other sets of individuals.
It includes:

- Management
- HR Department
- Assets

ICT boundaries:

ICT provides the means to connect the members of a community across geographical or institutional boundaries.It also covers any product that will store, retrieve, manipulate, transmit, or receive information electronically in a digital form.
It Includes:

- Server, Server Rooms
- ISMS
- IT Systems and Labs

Physical Boundaries: A Physical boundary represents the physical perimeter that surrounds a set of assets that are owned and governed by an organization.
It includes:

- University Building and facilities.
- Infrastructure

Interfaces:

The organizational interfaces can be identified on two different levels in the organization: the management level and the operational level. At the operational level, several different organizational interfaces exist. The organizational interface on the management level consisted of how the work was organized.

Management level	**Operational level**
Finance(Bank Servers,Banking Apps)	IT security Department(Database of the University)
HR department(Database of the university)	Student Portal/eCampus(Database, University Websites)
Marketing Department(University Website)	Campus Security(Surveillance Application)

The scope of the St. Poelten University of applied sciences ISMS applies to the provision that are fully integrated to deliver the complete process and management of the Information security functions including:

- Student/Employee data confidentiality
- 24*7 Uninterrupted business process
- Ensure security of confidential payment details and other financial records.
- Confidentiality of Management and Business,marketing strategies
- Proper maintenance, Uninterrupted access to Student Portal and Student Portal

The scope also includes staff and assets that support these functions based at the head office at St. Poelten University of applied sciences. These services are provided from its Head Office in St.Poelten.

Topic: Policy

NOTE: For the Policy, please refer to File

“Policy.pdf”

Topic: Detailed description of information security roles, responsibilities and tasks

In accordance with existing laws, regulations, and contracts, the administration is in charge of administering St. Pölten University's values effectively and satisfactorily.
The Chairman is in charge of all aspects of information security within the company, including IT security and people security.

Chief Security Officer (CSO)

Information security is primarily the responsibility of the Chief Security Officer (CSO).

The CSO is responsible for executing and overseeing, among others, the following duties:

- **Day-to-Day Operations**: Implementing and overseeing strategies to assess and mitigate risk, safeguarding the corporation and its assets, and crisis management.
- **Security**: Developing, implementing, and maintaining security processes and policies, identifying and reducing risks, and limiting liability and exposure to informational, physical, and financial risks.

- **Compliance**: Working with a legal/compliance team, or being independently responsible for ensuring the company complies with local, national, and global regulations, especially in areas like privacy, health, and safety.
- **Innovation**: Conducting research and executing security management solutions to help keep the organization safe.

System owner

The system owner is in charge of determining the needs for purchases, developing and maintaining information and associated information systems, and consulting with the IT department. Every system and kind of information needs to have a clear owner. The owner of the system must specify which users or user groups have access to the information and what constitutes an approved use of this information. A separate document must contain a description of the system ownership [REF]

System administrator

System administrators are in charge of managing the data that has been given to St. Pölten University by third parties as well as the university's own information systems. There may be one or more devoted system administrators for each sort of information and system. These are in charge of safeguarding the data, including the implementation of systems for access

control to guarantee confidentiality and the execution of backup procedures to prevent the loss of important data. In compliance with the security policy, they will also continue to administer and maintain the security systems. One or more system administrators are required for each system. This needs to be recorded.

Users

Workers and students are dependable for getting familiar and complying with St. Pölten University's IT controls. Questions regarding the administration of different sorts of data ought to be postured to the system owner of the significant data, or to the system administrator.

Consultants and contractual partners

Contractual partners and contracted consultants must sign a confidentiality agreement prior to accessing sensitive information.(e.g. Third-party funds that finance research projects) The System owner is responsible for ensuring that this is implemented.

Topic: Risk Management

Prioritized risks

1. Ransomware Attack
2. Attacks on door Access control
3. Usage of External devices (eg:- USB stick)

1. Ransomware Attack

Ransomware is often sent through phishing emails that contain malicious codes. Such malicious codes are designed to deny the organization from accessing the important files. By encrypting these files and demanding ransom payment to get a decryption key. As a university, a lot of confidential data will be there in the database, for example student personal information, employee information, payment information of students and employees, university infrastructure documents.

Treatment Strategies

- Blockdown payloads from launching by using anti-malware softwares.
- Regular backup of file to external storages like S3, Cloud storages.
- Making awareness about possible ransomware attack methods.

2. Attack on door access control

Most of the university door access is controlled by RFID cards. If an unauthorized person gets access to information stored in RFID cards, they can easily copy the data into another card to generate a replica.

Treatment Strategies

- RFID Blocking wallets are the best method to avoid RFID theft.
- Making aware of proper usage of RFID devices.
- Making aware of social engineering, to avoid manipulations.

3. Usages of external devices

As the University is available 24*7 Anyone with a campus card can enter and an unauthorized person can also enter to make use of the chance. In such cases all the labs and systems are available for use. This is the first scenario that an attacker can use external devices to inject malwares to systems. The other scenario is someone can manipulate the actual authenticated person(student/employee) to use external devices in the premises of the University, and thereby inject malware to the system.

Treatment Strategies

- Centralized management policy to manage the client system like (Active active directory and Policy).
- Usage of strong Anti-malware softwares.
- Making aware of social engineering.