ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

Information Security Policy				
Document No: 12567	Status: Approved	Classification: Public	Issue Date: 15.10.2022	Next Review Date:15.10.2023

Information Security Policy

Revision: v1.2
First published:13.10.2022
Updated:15.10.2022
Prepared by: Information security department
Classification: Public

Revision History:

Revision No.	Date	Changes
v1.0	13.10.2022	First Draft
v1.1	14.10.2022	First approved version
v1.2	15.10.2022	Modified Policy Statements

Information Security Policy				
Document No: 12567	Status: Approved	Classification: Public	Issue Date: 15.10.2022	Next Review Date:15.10.2023

1.Table of contents

Information Security Policy				
Document No: 12567	Status: Approved	Classification: Public	Issue Date: 15.10.2022	Next Review Date:15.10.2023

2.Introduction

2.1 Background

St. Pölten University of Applied Sciences is committed to safeguard the confidentiality, integrity, and availability of all physical and electronic information assets of the institution to ensure that regulatory, operational and contractual requirements are fulfilled. The overall goals for information security at St. Pölten University of Applied Sciencesare the following:

- Ensure compliance with current laws, regulations, and guidelines.
- Comply with requirements for confidentiality, integrity and availability for St. Pölten University of Applied Sciences 's employees, students and other users.
- Establish controls for St. Pölten University of Applied Science's information and information systems against theft, abuse and other forms of harm and loss.
- Motivate administrators and employees to maintain the responsibility for, ownership of and knowledge about information security, in order to minimize the risk of security incidents.
- Ensure that St. Pölten University of Applied Science's is capable of continuing their services even if major security incidents occur.
- Ensure the protection of personal data (privacy).
- Ensure the availability and reliability of the network infrastructure and the services supplied and operated by St. Pölten University of Applied Science.
- Comply with methods from international standards for information security, e.g. ISO/IEC 27001.
- Ensure that external service providers comply with 's information security needs and requirements.
- Ensure flexibility and an acceptable level of security for accessing information systems from offcampus.

2.2 Security strategy

St. Pölten University of Applied Science's current business strategy and framework for risk management are the guidelines for identifying, assessing, evaluating and controlling information related risks through establishing and maintaining the information security policy (this document).

Information Security Policy				
Document No: 12567	Status: Approved	Classification: Public	Issue Date: 15.10.2022	Next Review Date:15.10.2023

It has been decided that information security is to be ensured by the policy for information security and a set of underlying and supplemental documents. In order to secure operations at St. Pölten University of Applied Science even after serious incidents, St. Pölten University of Applied Science shall ensure the availability of continuity plans, backup procedures, defence against damaging code and malicious activities, system and information access control, incident management and reporting.

The term information security is related to the following basic concepts:
• Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
• Integrity: The property of safeguarding the accuracy and completeness of assets.
• Availability: The property of being accessible and usable upon demand by an authorized entity.

Some of the most critical aspects supporting St. Pölten University of Applied Science 's activities are availability and reliability for network, infrastructure, and services. St. Pölten University of Applied Science practices openness and principles of public disclosure but will in certain situations prioritize confidentiality over availability and integrity.
Every user of St. Pölten University of Applied Science 's information systems shall comply with this information security policy. Violation of this policy and of relevant security requirements will therefore constitute a breach of trust between the user and St. Pölten University of Applied Science, and may have consequences for employment or contractual relationships.

3 Scope

All data processing and information gathering will be done in compliance with current Austrian law. This policy outlines how the University will protect electronic data contained in:

- Key Business System data and information.
- The University's IS/IT infrastructure
- Security of information held in electronic form on any University computer.

And is processed or used by:

1. University Staff and suppliers who have access to or administer the University network or IT systems.

2. External users, agents, and guest users authorised to use the University network or IT Systems.
3. Individuals who process key data and information within Key Business Systems.

4. Policy Framework

4.1 POLICY Statements

St. Poelten University of Applied Sciences is committed to understanding and effectively managing risks related to Information Security to provide greater certainty and confidence for our securityholders, Students, employees, suppliers and for the communities in which we operate. Finding the right balance between information security risk and business benefit enhances our business performance and minimizes potential future exposures.

The policy of St. Polten University of Applied Sciences is to ensure:

- Information will be protected against unauthorized access.
- Confidentiality of information will be maintained.
- Information will not be disclosed to unauthorized persons through deliberate or careless action.
- Integrity of information through protection from unauthorized modification.
- Availability of information to authorized users when needed.
- Information security training must be completed by all staff.
- All suspected breaches on information security will be reported and investigated.

4.2 Staff Security

Employer responsibilities Guide You are responsible for ensuring the safety and security of your workers. One way of safeguarding your staff is to carry out a staff risk assessment and then take action to minimize those risks. Such action may include introducing monitoring technology, eg: CCTV surveillance, and by providing certain information security like providing proper confidentiality to their profile and confidential data stored in the university database

4.3 Awareness and Training

Security awareness training is a strategy used by IT and Security professionals to prevent and mitigate user risk. These programs are designed to help users and employees understand the role they play in helping to combat information security breaches. University is providing these awareness training for all staff and students at the time of joining the university.

4.4 Access Controls

In the fields of physical security and information security, access control is the selective restriction of access to a place or other resource, while access management describes the process. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization. Access is ensured in every aspect at the university. Eg: for entering the university there are access controlled systems that monitors who is entering and leaving the university building. Also for the digital premises proper authentication is ensured for the university websites.

4.5 Computer Network Security

Network Security protects your network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection. The University provides all kinds of security for the systems and network including firewall protection, database security etc.

4.6 Information Risk Management

A detailed analysis of all FH St Polten information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats – internal or external, natural or manmade, electronic and non-electronic-- that affect the ability to manage the information resources. All the assessments shall be submitted to the SIRO for review.

4.7 Information Classification

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. The information must be classified according to the most sensitive detail it includes. All the information assets of FH St Polten shall be classified according to this policy. The classification has to be documented.

Confidential information: Confidential Information is very important and highly sensitive material. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.

Internal information: Internal Information is intended for unrestricted use within FH St. Polten, and in some cases within affiliated organizations such as the University business partners. This type of information is already widely-distributed within FH St. Polten, or it could be so distributed within the organization without advance permission from the information owner.

Public information: Public information has been specifically approved for public release by designated authorities of the University.

4.8 Handling Software Threads

All software packages that reside on computers and networks within the University must comply with applicable licensing agreements and restrictions and must comply with the University's acquisition of software policies.

4.9 Internet, e-mail, and Computer use

The use of University automation systems, including computers, printers, and all forms of Internet/intranet access, is only for authorized purposes.

4.10 System Monitoring

The corporate IT System shall be monitored for system use and access. An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. The system monitoring measures shall be compliant with the GDPR and Human rights.

4.11 Business continuity and disaster recovery

The objective of a disaster recovery plan is to ensure that you can respond to a disaster or other emergency that affects information systems and minimize the effect on the operation of the business. Periodical backups of valuable data shall be ensured. The disaster recovery cell shall be formed to facilitate the rapid restoration of data after the occurrence of any disaster. Disaster management alerts shall be implemented.

Goals of disaster recovery plan

- To minimize interruptions to normal operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To train personnel with emergency procedures.
- To provide for smooth and rapid restoration of services.

5. Roles and Responsibilities

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.

5.1 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.

5.2 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]

5.3 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.

5.4 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.

5.5 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.

6 DISTRIBUTION AND IMPLEMENTATION

6.1 Distribution plan

A set of information security policies should be defined, approved by management, published, and communicated to employees and relevant external parties.These policies should be communicated to employees and relevant external parties in a manner that is relevant, accessible, and understandable to the intended reader, for example, as part of a "information security awareness, education, and training program."

University distribute security policies and track acknowledgement for two primary reasons.

1) The first point to make is that written security policies define "rules of behavior" for how users interact with data and systems.Given that the majority of data breaches are the result of human error, this appears to be a reasonable way to reduce risk.
Employees who do not understand how to use systems securely increase the potential risk dramatically. Acceptable Use Policies are the most common way to express these "rules of behavior."

2) Organizations are frequently encouraged to modify their information controls in response to "the size and scope of the business" or "the results of a risk assessment."

Variations of these statements can be found in HIPAA/HITECH and GLBA regulations.

This essentially means that the organization has the ability to add or remove controls based on a risk assessment or other business justification.

6.2 Training Program

The Personal Information Security Certification (PISC) is a set of ten principles for information security awareness. These constitute a "Common Body of Knowledge" that every computer user must be familiar with in order to protect themselves and their organization.

1: Your Role in Information Security
2: Information Classification
3: Information Access Control
4: Use of Electronic Mail
5: Use of Internet and Web
6: Use of Personal Computer Systems
7: Physical Security Principles
8: Secure Communications
9: Security Policies
10:Reporting Incidents

7 Monitoring and reporting

All changes will be monitored once policy roll-out to the University IT infrastructure. Active patching teams, as defined in the Roles and Responsibilities, must compile and maintain reporting metrics that summarize the results of each patching cycle. These reports will be used to assess the current level of risk and evaluate the current patching levels of all systems. On request, these reports must be made available to Information Security and Internal Audit.

Enforcement:

The ultimate responsibility for implementing and enforcing this policy rests with all employees at University Information Security, and Internal Audit may conduct random

assessments to ensure policy compliance without notice. Any system found in violation of this policy must be corrected immediately. Violations will be recorded in the University's issue tracking system, and support teams will be sent to resolve the problem. Failure to adhere to policy on multiple occasions may result in disciplinary action.