INFORMATION SECURITY POLICY

IT University of Copenhagen
Version 2.0
September 2018

This document is intended for all staff, students, associated businesses, suppliers, consultants and collaboration partners of the IT University of Copenhagen

© IT Department at the IT University of Copenhagen
Rued Langgaards Vej 7
2300 Copenhagen S

All rights reserved.
# Table of Contents

1 Introduction
   1.1 Purpose 3
   1.2 Scope 3

2 Organization and Responsibilities 4

3 Security Level
   3.1 Risk impact assessment 5
   3.2 Information asset security 6
   3.3 Network and operational security 6

4 Access management 7

5 External suppliers and collaboration partners 7

6 Security incidents and contingency planning
   6.1 Security incidents and breaches 8
   6.2 Contingency management 8

7 Information security awareness 9

8 Information Security Management System (ISMS) governance 9

Appendix 1 – Version history 10
1 Introduction

The “Information Security Policy” defines the governing framework for information security at the IT University of Copenhagen, while enabling the three core values: Direction-finding, Forthcoming and Accountable.

It is the aim of the IT University of Copenhagen (ITU) that both current and future levels of information security, is to:

- Asses and implement an adequate level of information security, both technical and organisational
- Ensure that information security and usability supports one another to achieve the best possible balance
- Maintain a level of user awareness that ensures, that the adopted rules and regulations are known throughout the organisation
- Strive to uphold legislative and organisational demands, when entering into contractual obligations with collaboration partners, suppliers and other relevant parties

ITU is utilizing the ISO 27001 framework for information security, as a means to govern and enable the secure use of hardware, software and data (also known as information assets), for both staff, students, associated businesses, collaboration partners, consultants and suppliers of ITU, as well as to ensure a uniform level of information security across the whole of ITU.

To support the governance and compliance surrounding information security at ITU, ITU has established:

- The IT Security Committee, consisting of representatives from management and from the IT Department, to steer ITU in the right direction
- An Information Security Management System (ISMS) as a method to govern the information security at ITU, and that contains policies, guidelines, manuals and procedures for the protection of information assets

The Information Security Policy is approved by the IT Security Committee at ITU.

---

1 ISO27001:2013, ‘Standard for information security’

2 An information asset is a body of knowledge that is organized and managed as a single entity. It is any data, device, or other component of the IT environment that supports information management related activities. Assets generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and confidential information
1.1 Purpose

The purpose of this policy is to ensure that:
- Staff and students can perform as required with a high level of quality and efficiency in their use of Information assets
- Information security is a natural part of the organisations approach to processing and handling information assets
- Individuals feel confident in entrusting their data to ITU, in the knowledge that ITU has established the necessary technical and organisational means to secure data
- Legal and contractual requirements can be met

1.2 Scope

The Information Security Policy applies to all of ITU's information assets, which is any information assets belonging to the ITU, regardless of how and where this information asset is stored and/or communicated. The policy also applies to information assets that does not belong to the ITU, but that the ITU can be held responsible for, for instance as a Data Processor.

The Information security policy applies to all staff without exception, both permanent employees and temporary employees as well as all students and guest students with access to information and information systems at ITU. Unless otherwise specified, all these persons are referred to as 'IT users' or 'users'. The Information Security Guidelines supplements the Information Security Policy, as well as other applicable ISMS documentation.

The Information security policy applies also to all alumni, associated businesses, suppliers, consultants and collaboration partners with physical or logical access to the ITU's systems and data, or to whom the ITU has outsourced parts of the IT operation.
2 Organization and Responsibilities

At ITU the responsibility of maintaining the adequate level of information security is an organisational task, that we take seriously.

To ensure that the handling of information assets including the processing of regular data and sensitive personal data, is in compliance with the ITU Information Security Policy as well as legislative requirements, it is important to organize the organization in a way that makes it a natural practice to comply with information security rules. This requires an anchorage in top management that supports and encourages information security. The IT Security Committee at ITU consists of members of the Executive Management, Department Heads and the CISO.

Department management must work for a culture where accountability in relation to processing and handling information assets falls naturally to everyone. This is partly done by ensuring that all users:

- Have the necessary knowledge of information security rules and guidelines
- Know where to find relevant documentation
- Receives the adequate awareness training continuously

It is the responsibility of every employee, student, collaboration partner and supplier to familiarize themselves with the relevant information security material made available in the ISMS (see section 8). All users with access to ITU's information systems must be aware of their responsibilities and roles in connection with ITU's information security so that the risk of human errors, theft, fraud and misuse of data is minimised. This includes staying aware of the rules and guidelines at ITU that applies to the work a user performs, as well as knowing where the current documentation can be found (see section 8).

A generic description/role distribution of the delegated Information security related responsibilities are listed in the Information Security Guidelines.
3 Security Level

Maintaining and expanding an adequate security level is essential for ITU to appear credible both nationally and internationally.

ITU is, at its core, an international organisation who collaborates with partners worldwide, while inviting students in from all over the world. At the same time national and EU legislation such as the GDPR\(^3\) stipulates technological and personal data processing demands, which must be adhered to. It is therefore important that the security level at ITU is balanced against the flexibility and dynamics of our day-to-day work, without conflicting with legislative demands.

At ITU, credibility is obtained by ensuring that data is accessible while treated with the necessary confidentiality and that the treatment of data and approved transactions is complete, precise and timely while preserving its integrity.

3.1 Risk impact assessment

Based on a systematic identification and assessment of risks through a Risk Impact Assessment process, ITU wants to maintain and continuously expand an information security level that ensures the appropriate level of confidentiality, integrity and accessibility for a given information asset.

The Risk Impact Assessment process is a continued cooperation between the organisation and the IT department, where the requirements set out in ISO 27001 are met, while addressing relevant consideration for the IT business risks, along with the financial situation and resources as well as compliance with specific legal requirements such as privacy impact assessment (DPIA) and contractual requirements.

Subsequently as part of the Risk Impact Assessment, all assets must be classified and labelled to support compliance with GDPR.

The Risk Impact Assessment for each relevant information asset is updated annually, as well as in the event of any major changes to the asset or its use, allowing the Management to keep up-to-date on the current risk situation.

ITU’s definition of classification is stated in the Information Security Guidelines.

---

\(^3\) GDPR: General Data Protection Regulation (EU) 2016/679 of the EU-Council of 27 April 2016.
3.2 Information asset security

The use of information assets, whether it be IT systems or data, is a vital part of the ITU. Assets must be protected from theft and loss to the best of ITU’s ability, which will include:

- Regular backup routines to ensure against loss of data
- Endpoint protection from virus, malware, ransomware etc.
- 2 factor VPN solution
- Encryption
- Update and patch procedures for software and hardware
- Physical security measures when applicable to secure rooms and information assets from unauthorised physical access as well as physical damage and disruptions

3.3 Network and operational security

Security measures must be in place to safeguard against unauthorised access to, or loss of availability to networks, systems, endpoints and data. Procedures must be established to ensure due diligence on patch, update and change management. As well as procedures to ensure that the necessary logging and monitoring is established.

ITU will continuously search for, research and evaluate new security related knowledge and tools in order to provide the adequate security level that fits the organization’s needs.
4 Access management

At ITU only authorized persons may have access to confidential or privacy data.

At ITU, we have formal internal procedures in place to manage both the granting of access, approval of access and revoking of access rights for staff, students, suppliers and collaboration partners, in order to ensure that a given user at any given time will have access only to the IT systems and data that he or she is authorised to.

5 External suppliers and collaboration partners

At ITU, we choose to engage with external suppliers and collaboration partners, who handle information security and privacy regulation professionally and take their accountability seriously.

Associated businesses, collaboration partners and suppliers with physical or logical access to the ITU’s systems and data, or to whom the ITU has outsourced parts of the IT operation, is a part of the natural organizational day-to-day way of doing business with global collaboration in mind.

Suppliers and collaboration partners that acts as a Data Processor must sign a data processor agreement, including a detailed instruction, prior to processing any personal data, as well as comply with a mutually agreed audit plan.

Associated businesses, collaboration partners and suppliers that does not act as a Data Processor, must be aware of and comply with the relevant ITU policies applicable at any time. As part of the ISMS there is a generic Information Security manual for external users, that applies to associated businesses, external collaboration partners and suppliers, unless specific instructions have been issued.

If ITU acts as a Data Processor, the ITU will likewise comply with regulatory rules set out for Data Processors in the GDPR, as well as the agreed terms and instructions given by a Data Controller.
6 Security incidents and contingency planning

At ITU we believe, that only if we, as an organization, stand vigilant together, can we stay ahead of wrongdoers.

At ITU, all users have a responsibility to help keep ITU as secure as possible. It is therefore expected that every user proactively respond to security incidents and vulnerabilities, by informing the IT helpdesk at IT@itu.dk.

6.1 Security incidents and breaches

When security incidents or breaches occur, they are handled and corrected depending on their severity. Serious breaches are analyzed to continuously improve IT security.

Where legal consequences may occur, evidence must be collected, stored and presented so that the ITU can ensure, that the evidence is complete and reliable.

All security incidents and breaches are documented, and reports are evaluated by the IT Security Committee at ITU.

6.2 Contingency management

Contingency management is implemented as an ongoing task with two purposes: to limit the consequences of accidents and errors in the ITU’s information assets

1. To restore the operation through a combination of preventive and remedial measures.
2. ITU emphasises well-planned physical security and monitoring of buildings, technical installations and IT equipment to avoid accidents and errors to the greatest extent possible.

The contingency plans must be updated and tested regularly, as a minimum at annual security drills.
7 Information security awareness

At ITU we acknowledge, that in order to obtain the desired level of information security, we must correspondingly raise the level of user awareness.

ITU prioritises the task of continuously keeping a constant level of user awareness in regards to information security. Awareness training is to be conducted at regular intervals throughout the organisation, and is part of the annual cycle of information security government.

For a department manager as well as a user, engaging in and prioritizing awareness training is an essential part of a natural practice to comply with information security rules and guidelines.

8 Information Security Management System (ISMS) governance

At ITU, we aim to keep the ISMS governance as dynamic and up-to-date as possible, while critically taking the ever-changing risks and trends into consideration.

The ISMS at ITU contains the governance framework and documentation for how information security is to be conducted at ITU, to preserve confidentiality, integrity and availability in our information assets. The ISMS will be updated and maintained on a regular basis.

- The following documentation will gradually over the next year make up the ISMS:
  - Information Security Policy (present document) approved by the IT security committee
  - A Statement of Applicability (SoA) document approved by the IT security committee
  - Information Security Guidelines (compiled version)
  - Information security policies and manuals for specific topics or to specific target groups when relevant (excerpts from the “Information Security Guidelines”)
  - Standard Operation Procedures (SOP)’s from the GDPR compliance program
  - A system overview, including risk scores
  - Risk Impact Assessments for all identified systems
  - System owner responsibility and role description
  - A plan for the annual cycle of information security government, including:
    - Awareness
You can find material relevant for all of ITU on the ITU intranet:
- ABC\Information Security or Guides\Information Security
- ABC\GDPR or Guides\GDPR

For documentation relevant for a specific department, e.g. procedures, refer to the specific department.

**Appendix 1 – Version history**

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Performed by</th>
<th>Changes</th>
<th>Approved by</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>31st of August 2010</td>
<td>Anne Hedegaard Tvedebrink</td>
<td>The IT Security Policy is approved by the IT Security Committee.</td>
<td>ITS</td>
</tr>
<tr>
<td>1.1</td>
<td>11th of October 202</td>
<td>Anne Hedegaard Tvedebrink</td>
<td>The IT Security Policy have been reviewed and approved by the IT Security Committee.</td>
<td>ITS</td>
</tr>
<tr>
<td>1.2</td>
<td>27th of January 2015</td>
<td>Mickie Friebe</td>
<td>The IT Security Policy have been reviewed and approved by the IT Security Committee. Minor changes concerning change from DS484 to the use of ISO27001:2013.</td>
<td>ITS</td>
</tr>
<tr>
<td>1.3</td>
<td>11th of November 2015</td>
<td>Peter Smidt</td>
<td>The IT Security Policy have been reviewed and approved by the IT Security Committee. Corrections concerning references to ISO27001/2 sections.</td>
<td>ITS</td>
</tr>
<tr>
<td>2.0</td>
<td>12th of September 2018</td>
<td>Lilian Schelde Baunbæk</td>
<td>The IT Security Policy have been replaced by the Information Security Policy. Reviewed and approved by the IT Security Committee.</td>
<td>ITS</td>
</tr>
</tbody>
</table>
IT University of Copenhagen
Rued Langgaards Vej 7
2300 Copenhagen S

Opening hours:
Monday - Friday
10 AM to 13 PM
Wing 2C

it@itu.dk