IT UNIVERSITY OF COPENHAGEN

INFORMATION SECURITY POLICY

for

IT University of Copenhagen

Version 2.4 – August 2025

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

Table of Contents

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:

- Assess and implement an adequate level of information security, both technical and organisational.
- Ensure that information security and usability support 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[1] framework for information security, as a means to govern and enable the secure use of hardware, software and data (also known as information assets[2]), 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 Security and Compliance Board structure, consisting of 3 tiers with representatives from executive management in Tier 1, representatives from the IT Department, Management Secretary, HR, SAP, and Faculty in Tier 2, and CISO, Legal, Department Support and Learning Support in Tier 3, to steer ITU in the right direction. Refer to Appendix B for the hierarchical structure.
- An Information Security Management System (ISMS) is a method to govern the information security at ITU, that contains policies, guidelines, and procedures for the protection of information assets.

The Information Security Policy is approved by the Security and Compliance Board Tier 1 level at ITU.

[1] ISO27001:2022, '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 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 ITU's **information assets**, which is any information asset 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 guidelines listed in "Information Security at ITU" supplements the Information Security Policy, as well as other applicable ISMS documentation.

The Information security policy applies also to all **associated businesses, suppliers, external affiliated users[3]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 compliant 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 **Security and Compliance Board Tier 2** has been delegated a mandate to make and enforce several security and compliance decisions on behalf of the Executive Management at ITU. Tier 2 consists of members of Department Heads, Faculty, Legal, and CISO.

[3] External Affiliated user is a user that is not a permanent member of staff but needs access to infrastructure and/or systems. I.e. an IT supporter or administrator from a Supplier, a consultant, a visiting Scholar, a temporary worker.

It is a responsibility for the **Management at ITU** to 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.
- are encouraged to use the necessary time to improve security skills.

Furthermore, **Management** must ensure that staff whose tasks will include the handling of sensitive and/or confidential information is made aware of their special responsibility and role in connection with this work.

It is the responsibility of every **employee, student, external affiliated user, 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 Organisation (Appendix A)

2.1 Termination of employment

Procedures must be in place to ensure that all IT assets are returned, and rights are revoked at the termination of employment of any ITU employee. This applies to permanent as well as temporary staff. This also applies to students who have been granted extraordinary access to the ITU's information systems. Following termination of employment, a user is still required to adhere by the rules of confidentiality.

2.2 Violation of the Information Security Policy

Users who violate or repeatedly fail to comply with the Information Security Policy or its pertaining rules will become subject to disciplinary action in accordance with the ITU's rules and staff policy applicable.

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 FIKS[4], GDPR[5] and AI Act[6] 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 (PIA) 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 evaluated annually, as well as in the event of any major changes to the asset or its use. Furthermore, the Risk Impact Assessment evaluates individual risks based on their probability and impact on the information asset, allowing ITU to register and track each risk including how the individual risk is handled or mitigated, thereby enabling the Management at ITU to keep up to date on the current risk situation.

[4] FIKS, previously known as URIS, consists of recommendations about identifying and protecting research, knowing collaboration partners, and protecting the institution, the employees and students.

[5] GDPR: General Data Protection Regulation (EU) 2016/679 of the EU-Council of 27 April 2016.

[6] AI Act: Artificial Intelligence Act (EU) 2024/1689 of the EU-Council of 13 June 2024.

ITU has approved the following data classification:

Classification	Definition
Public information	Information that anyone can access or be given access to by request. For instance, information found on/in itu.dk, publications, brochures, information on "ITU Student" etc.
Users own contact information	Information used by an individual when entering into a contract or license agreement, and where this information is controlled by a vendor. This classification can only be used when no other kind of personal data is exchanged.
Internal information	Information that is only to be communicated internally and is necessary to perform day-to-day operation. Access requires an ITU user account. For instance, information available on the intranet, internal mail, etc.
Confidential data	Information that is restricted to relevant ITU users, be it confidential business information (strategies, budgets, contracts, research results, etc.) or personal data that must be kept confidential about staff and students (employment terms, personnel cases, salary, CPR no's, MUS evaluations, student counsellor decisions, dialog between student counsellors and students, etc.). A breach of confidentiality may be harmful to the ITU or the party that the information concerns
Sensitive data	Information of a sensitive character that only the management of the ITU, or highly trusted IT users should have access to, including sensitive personal data about students and staff at ITU. For instance, information about health, sexual orientation, race and ethnicity, Trade Union membership, political opinion, religious and philosophical beliefs, genetic or biometric data. A breach of confidentiality may be very harmful to the ITU or the party that the information concerns.

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
- Forced MFA when accessing ITU's network, services and data
- 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 Travelling with ITU-devices

To minimize the risk to ITU's infrastructure and information assets during travels, all members of staff can temporarily borrow dedicated travel devices and have an option of setting up temporary accounts, when travelling to high-risk countries.

In addition, a guide for “Travelling with ITU Devices", containing requirements and advice can be found on the intranet.

3.4 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 to provide the adequate security level that fits the organization’s needs.

3.4 Cyber security

As a university with research data ITU face a higher risk of cyber-attacks with the intent to penetrate our network for information gathering purposes as well as the more common attacks like Ransomware, malware etc.

ITU aims to reduce the risk of cyber-attacks and protect against unauthorized exploitation by continuously striving to operate and maintain an adequate protection, detection, and resilience against cyber-attacks.

ITU partakes in the cooperation and sharing of relevant knowledge concerning cyber security across the Danish Universities, and the associated CERTs.

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.

When granted access to ITU's network and systems with an ITU user account, the individual external affiliated user is required to stay aware of and comply with the relevant and current ITU policies at any time, unless specific instructions have been issued. All relevant user policy information can be found in the pamphlet "Information Security when working at ITU" found on the intranet web site under "IT and campus facilities". The Head of Department responsible for entering into a contract, must ensure that an external affiliated user is introduced to this policy.

Associated businesses, collaboration partners and suppliers 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. In some cases, there is a need to sign a Non-Disclosure Agreement (NDA) as well.

Associated businesses, collaboration partners and suppliers that does not act as a Data Processer, may be required to sign a Non-Disclosure Agreement (NDA).

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 responds to security incidents and vulnerabilities, by informing the IT helpdesk at **IT@itu.dk.** Likewise, it is expected that all users take immediate necessary action if informed of a security vulnerability or security breach.

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 Security and Compliance Board Tier 2 level at ITU.

6.2 IT Contingency management

IT contingency management is implemented as an ongoing task with two purposes:

1. to limit the consequences of accidents and errors in the ITU's information assets

2. to restore the operation through a combination of preventive and remedial measures.

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 IT contingency plans must be evaluated and tested regularly, as a minimum at annual security drills.

6.3 Framework for Incident Management

ITU have an established standardized IT contingency plan, that provides a structured process for addressing 4 core incident types: Vulnerability management, Operational disruptions handling, Cyber-attack response and GDPR/personal data breaches.

7. Information Security awareness

*At ITU we acknowledge, that 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 regarding 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. Awareness training includes information on the intranet and in ReadIT and the annual security and compliance brush-up courses.

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 is part of the ISMS:

- Information Security Policy (present document) approved by the Security and Compliance Board
- A Statement of Applicability (SoA) document approved by the Security and Compliance Board
- Information Security at the IT University of Copenhagen (User policy) approved by the Security and Compliance Board

- Relevant Information security policies and guidelines for specific topics or to specific target groups
  - Backup Policy
  - Password Policy
  - Risk Assessment Policy
  - Private IT Equipment
  - Travelling with ITU devices
- Standard Operation Procedures (SOP)'s from the GDPR compliance program
- A system overview, including risk scores, maintained by CISO
- 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
  - Risk assessment
  - Contingency testing
  - Annual "state of the union" rapport
  - Annual management approval of core documentation

In addition, the ISMS will contain all relevant and documented security instructions and procedures at ITU. For example, documentation requested in the "System owner responsibility and role description" document and/or identified as necessary through risk impact assessments.

You can find material relevant for all at ITU on the ITU intranet:

- IT and campus facilities\Information Security when working at ITU
- Administrative support\ General Data Protection Regulation (GDPR)

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

Version history

Ver.	Date:	Performed by:	Changes:	Approved by:
1.0	31th of August 2010	Anne Hedegaard Tvedebrink	The IT Security Policy is approved by the IT Security Committee.	ITS
1.1	11th of October 2012	Anne Hedegaard Tvedebrink	The IT Security Policy have been reviewed and approved by the IT Security Committee.	ITS
1.2	27th of January 2015	Mickie Friebel	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.	ITS
1.3	11th of November 2015	Peter Smidt	The IT Security Policy have been reviewed and approved by the IT Security Committee. Corrections concerning references to ISO27001/2 sections.	ITS
2.0	12th of September 2018	Lilian Schelde Baunbæk	The IT Security Policy have been replaced by the Information Security Policy. Reviewed and approved by the IT Security Committee.	ITS
2.1	28th of August 2019	Lilian Schelde Baunbæk	The Information Security Policy have been reviewed and approved by the IT Security Committee. Apart from minor changes, a new Appendix A containing the Information Security organization has been added.	ITS
2.1	7th of October 2020	Lilian Schelde Baunbæk	The Information Security Policy have been annually reviewed and approved by the IT Security Committee. No changes.	ITS
2.2	4th of May 2022	Lilian Schelde Baunbæk	The Information Security Policy have been annually reviewed and approved by the IT Security Committee. Apart from minor grammatical changes, section 3.4 has been added.	ITS
2.3	1st of February 2023	Lilian Schelde Baunbæk	The Information Security Policy have been annually reviewed and approved by the IT Security Committee. The policy has been updated to reflect the new Security and Compliance Board structure. A new classification is added.	ITS

2.4	27th of August 2025	Lilian Schelde Baunbæk	The Information Security Policy have been reviewed and approved by the Security and Compliance Board Tier 2. The policy has been updated with minor changes to reflect procedural changes. Following new sections have been added: 3.3, 6.3 and Appendix B	SCB Tier 2

Appendix A Information Security Organisation at ITU

The following is a generic description/role distribution of the delegated information security related responsibilities at ITU.

Title	Allocation and explanation	Responsibilities
Person in charge of Information Security	The overall responsibility for Information Security lies with the top management. At ITU this is the Executive Management	The Executive Management approves the Information Security Policy and has the overall responsibility for security. The ITU Board of Directors is informed of the Information Security Policy.
The Security and Compliance Board (SCB)	The Security and Compliance Board is a 3-tier structure that consists of: Tier 1: Executive Management: ▪ University Director (Chairman of the board) ▪ Pro-rector ▪ Vice Chancellor Tier 2: Heads from the following departments: ▪ IT Department (Chair tier2) ▪ Legal (Chair tier 2) ▪ Department of Personnel ▪ Student Affairs and Program ▪ Head of a faculty ▪ DPO when needed Tier 3: ▪ CISO (Chair tier3) ▪ Legal representative ▪ Department Support representative ▪ Learning Support representative	Where: Tier 1 ▪ Ultimate risk owner ▪ Decision maker and approver ▪ Determines the risk appetite for ITU Tier 2 ▪ Mandated independent decision-maker on approved areas ▪ Qualification of material prior to Tier 1 assessment Tier 3 ▪ Processing of requests from ITU i.e., Legal and/or Security requirements ▪ New policies; guidelines; recommendation for decisions ▪ Preparation of threat and vulnerability assessments ▪ Incident reporting
Chief Information Security Officer (CISO)	The CISO is responsible for the Information Security function and is in charge of GRC processes. (Governance, Risk and Compliance)	The function is in charge of, e.g.: - Preparing and maintaining all Information Security related policies and manuals, including guidelines and procedures. - Preparing relevant security requirements to operationalise the Information Security Policy with appendices.

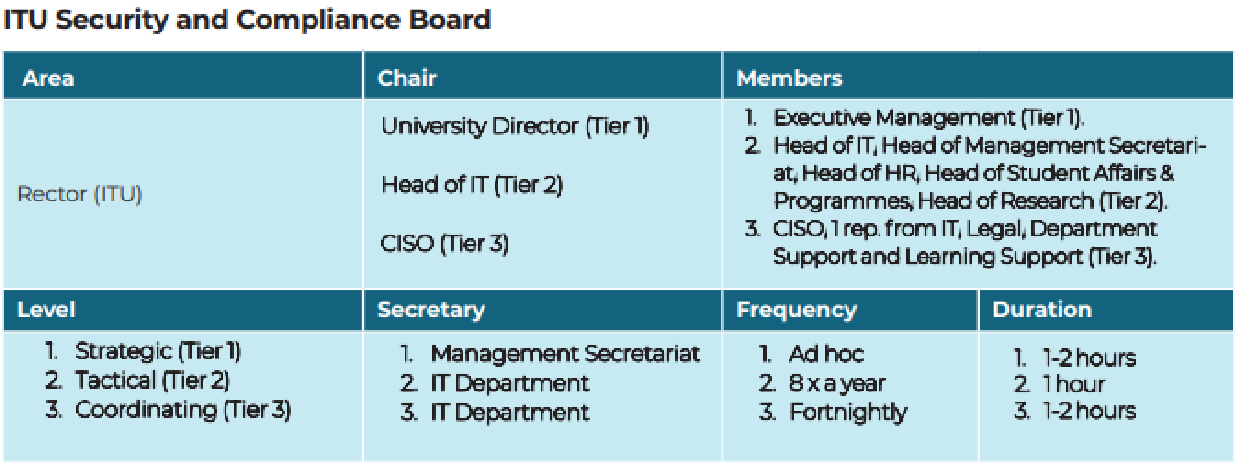
Title	Allocation and explanation	Responsibilities
		• Following up and reporting on important Information Security breaches to the Security and Compliance Board - Ensuring awareness of the Information Security Policy and Information Security in the organisation as a whole. - Coordinating the Information Security work and informing the organisation of important events and initiatives. - Keeping up to date about the general development within Information Security.
Function heads	Function heads of the following departments: ▪ IT Department ▪ Department of Finance ▪ Department of Personnel ▪ Student Affairs and Program ▪ Head of Research ▪ Head of Education ▪ Facilities Management ▪ Management Secretariat	It is the responsibility of the individual managers in the function – including the Management – e.g.: - To ensure that the Information Security Policy and the rules relevant to the individual manager's areas of responsibility are known and observed. - That the staff become aware of the need to follow the security policies and guidelines through education and development, and those policies and guidelines are observed. - To ensure that external affiliated users from associated businesses, collaboration partners and suppliers that the function enters into a contract with and that that has been given physical or logical access to the ITU's systems and data, know where to find relevant ITU security polices and guidelines. - That further documentation concerning security within the department's specific area is prepared as needed. - That a security/risk assessment is carried out before the installation of any new systems. - To coordinate the investigation if a security breach is discovered or suspected (the result is reported to the Information Security function). - To ensure that the guidelines for employment, introduction, regular assessment, change of work area and termination of staff are followed.
System Owner	System Owner is responsible for the Information Security of the system in question and must ensure: ▪ That internal users and external stakeholders have access to the information they need when they need it (accessibility). ▪ That the information is correct and complete (integrity).	System Owner is in charge of, e.g.: - Specifying Information Security requirements and preparing instructions for the individual systems. - Preparing detailed system documentation and support. - Approving acquisitions and system installation. - Classifying assets for type of data use. - Administering access and approvals of access, including supplier access. - Approving placement of critical assets. - Approving development and testing environments. - Approving business continuity plans. - Following up on Information Security events. - Describing related internal controls (electronic and manual).

Title	Allocation and explanation	Responsibilities
	▪ That sensitive information is protected from unauthorised access (confidentiality). System Owner tasks may be delegated in part or in full to e.g. the system administrator. The responsibility may not be delegated.	- Establishing additional tasks in connection with the system use, including authorisation, logging, internal controls, development and acquisition as well as contingency arrangements. - Preparing specifications that explicitly consider security issues before any system development /change /acquisition /update, with external assistance if needed. - Preparing a risk assessment pursuant to the relevant requirements. - Ensuring that the Change Management guidelines are followed in the event of system changes. - Ensuring that specific rules and procedures for the regulation and administration of access are available when the system is put into operation, and that these are in accordance with the fundamental requirements. - Authorising system access pursuant to the relevant guidelines. - Following up and reporting on security breaches to the Information Security function and thereby to the Security and Compliance Board. In situations where there is no separation of functions (authorisation/administration), other security measures will be used as compensation which will be implemented in the guidelines and specifically in rules and procedures for the system administration. If a system is classified as a critical system, the requirements outlined in the “System owner: Role description and responsibility (information asset owner)” must be documented.
Data owners	The data owner is responsible for the information security of the relevant data in the system and must ensure: ▪ That internal users and external customers have access to the information they need when they need it (accessibility). ▪ That the information is correct and complete (integrity). ▪ That sensitive information is protected from unauthorised access (confidentiality).	The data owner is in charge of, e.g.: - Classifying data - Preparing a risk assessment pursuant to the relevant requirements. For system associated data this assessment is made in cooperation with the system owner. - Ensuring that specific rules and procedures for the regulation and administration of access are available for data and systems, and that these are in accordance with the fundamental requirements. - Authorising the access to data pursuant to the relevant guidelines and ensuring that any security sensitive information activity can be traced to the person that has performed the activity. - Following up and reporting on security breaches to the Information Security function and thereby to the Security and Compliance Board.

Title	Allocation and explanation	Responsibilities
	Data owner tasks may be delegated in whole or in part. The responsibility may not be delegated.	In situations where there is no separation of functions (authorisation/administration), other security measures will be used as compensation which will be implemented in the guidelines and specifically in rules and procedures for the data administration.
Owners of physical assets	All physical assets will have an owner identified/assigned If the asset is subject to a hosting agreement this is taken into consideration in the agreement with the collaboration partner, e.g. by obligating the collaboration partner to make controls and follow-ups and report on these.	The owner of the physical asset is in charge of: - Preparing specifications for placement, arrangement, change etc. that explicitly consider security issues - with external assistance if needed. - Preparing a risk assessment pursuant to the relevant requirements. - Ensuring that specific rules and procedures for the regulation and administration of access are available when rooms/equipment is put into use, and that these are in accordance with the fundamental requirements. - Authorising room/equipment access pursuant to the relevant guidelines. - Following up and reporting on security breaches to the Information Security function and thereby to the Security and Compliance Board. In situations where there is no separation of functions (authorisation/administration), other security measures will be used as compensation which will be implemented in the guidelines and specifically in rules and procedures for the physical security and access administration.
IT management	The Head of IT and IT teamleaders.	The IT management is in charge of: - The IT operation. - Continuously describing and establishing internal procedures in support of the observance of the Information Security Policy with subsequent manuals and guidelines.
IT technical security	Employees within the IT Department, dedicated to technical security	IT technical security is in charge of: - Threat detection by means of monitoring, investigating and analyzing - Incident response - Securing and hardening infrastructure and servers - Protecting identities, endpoints and servers - Regular scans and testing
IT users	IT users are all staff and students without exception, both permanent employees and temporary employees of the ITU as well as all students and guest students with access to the ITU's information and information systems.	The individual IT user is responsible for: - Observing the Information Security Policy and the rules relevant to the individual user's tasks. - Reporting any security breaches or suspicion of such breaches to the user's immediate superior and to the Information Security function.

Title	Allocation and explanation	Responsibilities
Data Protection Officer (DPO)	The appointed DPO at ITU NB! this description relates to Information Security only.	The DPO at ITU has the following tasks: - Inform and advise ITU and the employees who carry out processing of their obligations pursuant to data protection provisions. - Monitor compliance with data protection provisions and with the policies in relation to the protection of personal data, including the assignments of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits. - Provide advice where requested in regards to data protection
Suppliers and collaboration partners	Suppliers and collaboration partners with physical or logical access to the ITU's systems and data, and suppliers and collaboration partners to whom the ITU has outsourced parts of the IT operation must also be aware of and comply with the policies applicable at any time at the ITU. Furthermore, a specific collaboration agreement must describe the supplier's/collaboration partner's security management.	Suppliers and collaboration partners are in charge of: - Ensuring that the ITU's Information Security Policy and the rules relevant to their area of responsibility are known and followed – most expediently by always reflecting the requirements of the ITU in their own security policies and rules. - Ensuring that staff with access to the ITU's information or information systems become aware of the need to follow the security guidelines specified for the relevant work through education and development. - Preparing further documentation concerning Information Security within the relevant area as needed. - Carrying out a risk/security assessment before any installation of new or modification of existing internal systems and components that may affect the ITU's information assets. - Coordinating the investigation when a security breach is discovered or suspected – this may be done by reporting to the Information Security function and thereby to the Security and Compliance Board.

Appendix B Security and Compliance Board hierarchy Structure



ITU Security and Compliance Board

Area	Chair	Members	
Rector (ITU)	University Director (Tier 1) Head of IT (Tier 2) CISO (Tier 3)	1. Executive Management (Tier 1). 2. Head of IT, Head of Management Secretariat, Head of HR, Head of Student Affairs & Programmes, Head of Research (Tier 2). 3. CISO, 1 rep. from IT, Legal, Department Support and Learning Support (Tier 3).	
Level	**Secretary**	**Frequency**	**Duration**
1. Strategic (Tier 1) 2. Tactical (Tier 2) 3. Coordinating (Tier 3)	1. Management Secretariat 2. IT Department 3. IT Department	1. Ad hoc 2. 8 x a year 3. Fortnightly	1. 1-2 hours 2. 1 hour 3. 1-2 hours