Information Security Policy

Reference: ISMS DOC 5.2

Organisation Issue No: HK_SOP_IT_SEC_V2.2

Organisation Issue Date: 13/01/2020

Revision History

Version	Modified on	Nature of update	Document ID
Ver 1.0	07.06.2018	Establishing an IT Security Policy	
Ver 1.1	04.03.2019	Updates on IT Security Policy and sent for approval to the Leadership group	
Ver 2.0	04.03.2019	Approved by leadership group	
Ver 2.1	13.01.2020	Updates on IT Security Policy; in compliance with ISO 27001 guidelines.	*HK_SOP_IT_SEC_V_2.1*
Ver 2.2	15.01.2020	Updates on IT Security Policy; - removed generic points and added email policy.	*HK_SOP_IT_SEC_V_2.2*
Ver 2.3	09.10.2020	Updates in the Sanctions section as recommended by the HR department	*HK_SOP_IT_SEC_V_2.3*

Kristiania University College is a non-profit university college founded in 1914,

located at

Prinsens gate 7-9,

0152 Oslo (Norway),

are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with Kristiania University College's goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations, for e-commerce and for reducing information-related risks to acceptable levels.

1. Policies are applicable to all the users that use the school's IT equipment and Information Systems, and/or are in a partnership with the school for sector-based cooperation and/or as support functions.

2. IT equipment consists of computers, mobile phones, network, software, data, storage media and other equipment of similar nature made available by Kristiania University College.

3. Information Systems are any form of physical or digital solutions provided to withhold any form of information pertaining to Kristiania University College. This information can be concerning students, employees, business partners or the school itself.

4. Users always have the responsibility to familiarize themselves with the contents of the policy document before using the IT equipment and keep themselves informed about the IT policies in use and any supplementary provision in effect.

5. IT Policies are available at http://kristiania.no/it for students, and over the intranet for the school's employees.

6. Contact information for the IT Department can be found at http://kristiania.no/it

Kristiania University College's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The *Risk Assessment, Statement of Applicability and Risk Treatment Plan* identify how information-related risks are controlled. CISO is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the Manual and are supported by specific documented policies and procedures.

Kristiania University College aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan.

All Employees of *Kristiania University College* and all the external parties:

i) any university or educational institution working in collaboration with Kristiania University College for research or educational purposes.

ii) any business partner supporting the university college for educational purpose or as an industry partner.

iii) any individual or organization associated with Kristiania University College to provide support in projects or any other activity pertaining to Kristiania University College's operations;

are expected to comply with this policy and with the ISMS that implements this policy.

All Employees and external parties will receive a copy of this document i.e. *Kristiania University College's Information Security Policy* at the time of employment (or retrospectively for employees already hired).

The following set of policies must be considered while accessing or utilizing any information resources of Kristiania University College.

Password Policy
Password is personal and should not be shared with others. When the users are notified to change their passwords, he/she should choose a password that is not easy to guess (should not contain personal information like your name, date of birth, car company etc.). In case, one suspects that their password has been compromised, it must be changed immediately.

Unauthorized use
Users has the responsibility to prevent any unauthorized access to their user accounts. If one discovers an event of unauthorized access, attempted such, or suspicion that outsiders have become aware of the password, this should be reported immediately to the IT department.

Users are responsible for any actions that are performed from their user account.

Unauthorized access
The user should not acquire or attempt to acquire access to systems or information he / she is not supposed to have access to; through to the school's IT systems. This also applies in the context of teaching or research.

Logout
To avoid any misuse or unauthorized access, it is important that the user secures access by logging out or using password-protected screensaver when he / she is not present, because unauthorized persons can otherwise easily access information during the user's absence.

Malicious Software
The user must ensure that software installed on the computer is not harmful to the computer or connected IT systems (viruses, malware, etc.). Essentially, software that is to be installed should be pre-approved by the IT department.

Instructions for use and routines
The user is obliged to familiarize himself with the user manuals, routines or matter of similar nature in such a way that the user reduces the possibility of ignorance; creating a risk of vulnerabilities, operational disruption or loss of data.

Accessing digital content
User must exercise caution when opening unknown files, e-mail attachments, files from unknown memory sticks, and the like. This is to prevent the equipment from being infected with malware such as viruses, spyware, Trojans and the like. If events do occur, the IT department must be notified as soon as possible.

Note: IT Department is free to block any services at its discretion, should it pose a security risk.

Use of non-standard services / solutions
It is not allowed to use services (for example: over the internet) that can hinder or disrupt normal operation of the school's IT Systems.

Use of IT equipment

- The user must avoid the use the IT equipment for activities that are not directly related to the school's activities.
- The user must ensure that the school's IT systems are not used for activities that violate the Norwegian law.
- It is not allowed to disconnect or move the school's stationary IT equipment without an agreement with the IT department. This does not apply to laptops that are in use by the employees.

Storage, backup and retention of data (for employees)

- Employees should ensure that work-related information is stored on the platforms (storage solution) provided by the school.
- Data that belongs to the school should be stored in such a way that it is backed up automatically. Be apprised that the data stored on the local computers is not backed up.
- Users are responsible to back up the data stored on their local computer.

Storage, backup and retention of data (for students)

- Students are responsible for their data themselves. However, the data in the learning portal and in other systems made available by the school are maintained in the same manner as the rest of the data pertaining to the school.
- Users are responsible to back up the data stored on their local computer.

Email Policy

- Email accounts provided by Kristiania University College are the school's property and must be strictly used for official purposes only.
- Since phishing is a very relevant and prevalent attack vector these days, it is vital that any observed phishing attack is reported to the IT support. If somebody accidently get exposed to such attacks, he should immediately change his password and contact IT Support for further assistance.
- Do not respond to requests for personal or sensitive information via email, even if the email seems to be from a trusted source.
- Use your discretion to verify the authenticity of the emails.
- Under no circumstances, use your email must contain any threats, language or images related to race, gender, age, sexual orientation, pornography, religious or political beliefs, nationality or disability.
- Information on persons or businesses must be retained or archived in a timebound manner and must have a reason to keep it due to some of the regulatory standards.

- Your email must follow the basic protocols of business emails like no use of slang, a signature, reply to all only whenever necessary, respond to emails in a reasonable timeframe.

Copyrighted material and licenses

- Use or sharing of the intellectual property shall only be done in accordance with the *Åndsverkloven* for intellectual property, etc. (Copyright Act).
- Downloading and/or sharing of the copyrighted material without an explicit approval from the owner of the copyrighted material is not allowed.
- It is not allowed to copy software and other right-restricted or licensed data (for example – fonts, pictures or similar material) from the school owned IT equipment.
- Software made available to the users by the school should always be used in accordance to the license agreement. Many of the licenses are meant to be used for educational purposes only and can thereby not be used privately or commercially. The IT department can clarify license terms; when needed.

Privacy

- Use of personal data must be in accordance with *The Personal Data Act*. The school's data privacy officer can guide in issues related to privacy.
- Registration of personal data must only be done after an agreement with the IT department. This applies regardless of purpose (research, studies, etc.).
- Storage media (such as CD / DVD discs, memory sticks, external hard drives and paper documents, etc.) containing personal information and / or confidential information should be handled and stored in secure way.
- Printouts containing personal information and / or confidential information, that is no longer needed by an employee, must be shredded. Obligations under this paragraph supplement confidentiality statements for those bound by them.

Use of private IT equipment

- The equipment is to be connected to the school network at own risk.
- School cannot be held responsible or liable for any piece of equipment that gets infected, stolen or affected by any means while using the school network or premises.
- Users are responsible to regularly update Anti-virus software and ensure that all the applications / OS are up to date with the all recent security patches.

Transparency and Data Disclosure

- Users shall not disclose any information about the employees or data belonging to a partner unless Norwegian laws or internal regulations are applicable.

- The IT department has the right to seek access to the individual user's reserved areas with the sole motive of 1) securing the IT systems functionality, or 2) checking that the user does not violate or has violated this regulation. It is assumed that such access is only sought when it is of critical to the operation of the school, and some special cases of suspicion. Permission for access to electronic mail shall be sought separately.
- If the IT department seeks such access, permission must be attained in advance from the *HR director* (for employees) or the *Student Administration director* (for students.
- If the use of computer, mobile phone or other end-user equipment, due to operational reliability or other considerations, is monitored by the IT department, this shall be stated with a mark on the device or otherwise.
- The IT department has a duty of confidentiality with regards to information they acquire about the user or the user's activity, with the exception of matters that represent a violation of these regulations.

Sanctions

- In the event of a breach, or suspicion of breach, of these provisions, the IT department may without further notice revoke user rights for up to 5 days.
- The HR director (for employees) and the *Student Administration director* (for students) can permanently revoke the user rights.
- There are sanctions that can be applied, in addition to the other provisions, at the school, or according to Norwegian law.

Should there be any ambiguity in the statements, appropriate clarifications shall be provided, and necessary changes will be made to the policy periodically as and when needed.

The consequences of breaching the information security policy are set out in the Organisation's disciplinary policy and in contracts and agreements with third parties. The ISMS is subject to continuous, systematic review and improvement. Kristiania University College has established a top-level management steering group called the Advisory Board , chaired by the *Chief Executive Officer (CEO) or a delegated body in collaboration with Chief Information Security Officer (CISO)* and including other executives/specialists/risk specialists to support the ISMS framework and to periodically review the security policy.

Kristiania University College is committed to achieving certification of its ISMS to ISO27001:2013.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, 'information security' is defined as:

Preserving

This means that management, all full time or part time Employees, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches (in line with the policy and procedures identified in Section 16 of the Manual) and to act in accordance with the requirements of the ISMS. All Employees will receive information security awareness training and more specialized Employees will receive appropriately specialized information security training.

the availability,

This means that information and associated assets should be accessible to authorized users when required and therefore physically secure. The computer network must be resilient, and Kristiania University College must be able to prevent, monitor, identify and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

Should there be a security incident threatening the availability of the information systems, these systems can be retrieved and re-instated using the backup solutions.

Confidentiality

This involves ensuring that information is only accessible to those authorized to access it and therefore to preventing both deliberate and accidental unauthorized access to Kristiania University College's information assets (any piece of information held digitally or on paper)

and its systems including but not limited to its network(s), website(s), extranet(s), Quality Assurance System, ERP system i.e. Business Central, Human resource management system etc.

i. Kristiania University College shall not disclose any information about the users or data belonging to a user unless Norwegian laws or internal regulations are applicable.

ii. The IT department has the right to seek access to the individual user's reserved areas with the sole motive of a) securing the IT systems functionality, or b) checking that the user does not violate or has violated this regulation. It is assumed that such access is only sought when it is of critical to the operation of the school, and some special cases of suspicion. Permission for access to electronic mail shall be sought separately.

iii. If the IT department seeks such access, permission must be attained in advance from the HR director (for employees) or the Student Administration director (for students), unless there are some special circumstances that demands immediate intervention. However, such special circumstances must be documented after the procedure.

iv. If the use of computer, mobile phone or other end-user equipment, due to operational reliability or other considerations, is monitored by the IT department, this shall be stated with a mark on the device or otherwise.

v. The IT department has a duty of confidentiality with regards to information they acquire about the user or the user's activity, except for matters that represent a violation of these regulations.

and integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorized modification, of either physical assets or electronic data. There must be appropriate contingency including but not limited to its *network(s), website(s), extranet(s), Quality Assurance System, ERP system i.e. Business Central, Human resource management system etc*. and data backup plans and security incident reporting.

Kristiania University College must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

The physical assets of Kristiania University College including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files. and information assets

The information assets

include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.).

of Kristiania University College.

Kristiania University College, and partners *i.e.*

i) any university or educational institution working in collaboration with Kristiania University College for research or educational purposes.
ii) any business partner supporting the university college for educational purpose or as an industry partner.
iii) any individual or organization associated with Kristiania University College to provide support in projects or any other activity pertaining to Kristiania University College's operations; have signed up to our security policy and have accepted our ISMS.

The *ISMS* is the Information Security Management System, of which this policy, the Information Security Manual ('the Manual') and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO27001:2013.

A *Security Breach* is any incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of Kristiania University College. Document Owner and Approval.

The CISO is the owner of this document and is responsible for keeping it up to date. The current version of this document is available to Human resources department, *Chief Information Security Officer (CISO), the Leadership Group and the Advisory Board.*

Post-approval, this document shall be available to all employees and students and shall be binding in nature - prior to use of any IT Asset of Kristiania University College,

and is published on intranet and Quality Assurance System - *Compilo*.