SECURITY POLICY	Document date	Possible Registration No.
	2018-06-11	V-2018-0491

Created by
KTH Security Manager

Security policy for KTH

The vision of the KTH Royal Institute of Technology (KTH) is to be a leading university of technology. KTH's security policy contributes to this by guaranteeing security conditions for continuity in the operations.

The security policy is updated and confirmed annually by the University Board of KTH, which through this provides support for the security work formulated in this policy. KTH's security policy shall serve as a guide and be communicated to employees and students.

The security work is intended to secure the life and health of employees, students and visitors. It also aims to prevent and limit damage to KTH's brand, property and environment through consistent actions in the event of disruptions and by maintaining continuity in vital operating processes.

The security work shall be based on current laws, ordinances, regulations and, where required, KTH's approved policies, ethical policy, quality policy, policy for sustainable development, HR policy, security policy and placement policy for KTH's donation capital, as well as guidelines, instructions and procedures that follow these policies.

The security policy is supported by guidelines and instructions for the governance of information and IT security, risk management, crisis management, physical security and systematic fire safety work. The steering documents in their respective form are addressed to employees and students, who are responsible for striving to realise them in applicable parts and working for safety prevention.

KTH's security manager is responsible for KTH's overall security work, collaboration with other authorities, training and information on preventive security for employees and students, coordinating security issues in the administration and with KTH's schools.

Information and IT security

KTH conducts systematic and risk-based information security work with support of a management system for information security (LIS). Standards that shall be observed are included in the information security standard ISO/IEC 27000. LIS enables management and measurement of the security level in the operations and that it is followed up. Information security consists of the three components: administrative security, physical security and IT security.

It is KTH's IT security manager who is responsible for coordinating, training in and informing about information and IT security issues at KTH, as well as developing procedures to prevent disruptions, the spread of harmful code and data infringement in the data networks, computers and computer systems from causing serious consequences.
Information security shall build on a reasonable level and at the same time ensure availability and reliability and guarantee that the right information is available to the right person.

KTH shall have internal procedures for identifying, reporting, assessing, managing and documenting incidents that can affect the security in the information processing that the authority is responsible for or in services that the authority provides to another organisation. KTH shall also

have processes for learning from such occurred incidents and taking action. KTH has prepared and develops processes and procedures that the authority needs to be able to meet the requirements on IT incident reporting.

Risk management

KTH shall take appropriate steps to limit risks and prevent damage or loss. Risk management in the security policy means the identification and evaluation of major security risks, such as threats, violence, terror, fire, etc. KTH shall evaluate the risks and calculate what costs the risks may entail. The results shall be compiled in a risk analysis.

KTH's security manager shall support the schools in the risk management work by providing advice and proposing appropriate measures that lead to preventing risks from arising, preventing damage and limiting its impact.

Crisis management

Every authority, the area of responsibility of which is affected by a crisis situation, shall take the steps necessary to manage its impact. KTH shall collaborate internally and externally with sensitivity to changes in society and our surroundings in order to confront and handle unforeseen events. KTH's crisis management capacity shall be high and the process clearly formulated at a central level and within the schools. Through training and practice, KTH shall develop and maintain skills for confronting and handling crisis situations that arise internally linked to the working environment and externally through outer influence. A crisis at KTH may be caused by fire, threats, violence or a serious accident. A crisis internally that affects KTH can be caused by natural disasters, serious epidemics, terrorist threats and collapsing IT systems. KTH's security manager is the convener of the crisis management group and assesses, together with the chairman of the crisis management group/administrative director, if the crisis management group shall be convened.

KTH's crisis management rests on three principles:

- The responsibility principle: means that the responsibility relationship with the President as the authority director shall be the same in a crisis as under normal circumstances.

- The equality principle: KTH's organisational structure and location in normal operations are the same as in a crisis. This means that the university administration shall serve as advisers, experts and collaborators with KTH's schools and that events are handled locally at the schools, until their crisis management group decides otherwise.

- The local principle: means that events shall be handled by the affected school and its responsible functions as long as the situation allows.

Physical security

Physical security at KTH shall serve to impede access for unauthorised personnel to KTH's premises with the aim of preventing a risk of insecurity for staff, students and KTH's visitors. In relation to protection requirements, it shall prevent the risk of damage, injury and loss by fire, water, climate – and environmental impact, vandalism, attack and unauthorised access. The physical security builds on effective and strategic security solutions that work in balance with KTH's openness and accessibility.

Systematic fire safety work

KTH shall, in a structured manner, plan, train, practise, document and control, as well as address and follow up the fire safety work in the organisation and collaborate with external organisations, owners, users and operations when activities are conducted within KTH or in direct connection therewith. In its capacity as an owner or holder of the right of use for a building or premises in which it conducts activities, KTH shall to a reasonable extent keep equipment to extinguish fire and save life, and actively work so that employees and students shall have knowledge of fire and its spread, in order to prevent, forestall and limit damage, injury, incidents and accidents as a result of fire.