POLICY	Valid from	Reference number
	01.07.2019	V-2019-0452
Decision-maker	**Date of decision**	**Responsible department**
University Board of Directors	11.06.2019	Sustainability, property and services

Security Policy

KTH shall provide a secure workplace and study environment. Security shall be based on efficient, strategic security solutions for an open and accessible KTH. KTH shall ensure that knowledge within the organisation with regard to physical security and data security is balanced with the operations KTH is tasked with performing and that security-related functions, authorities and responsibilities are clearly formulated.

Physical Security

KTH shall conduct systematic security activities to make it more difficult for unauthorised persons to access KTH's premises, so that any sense of insecurity among staff, students and visitors is prevented. Security work shall highlight risks within the organisation in order to ensure operational continuity, prevent damage to KTH's property and protect KTH's brand and sensitive operations.

KTH's crisis management capabilities shall be highly developed and our crisis management processes shall be clearly formulated. KTH shall conduct training and exercises to develop and maintain our capability to meet and deal with any crisis that may arise.

KTH shall systematically conduct and monitor fire protection work within the organisation and cooperate with external organisations, owners, users and businesses who conduct operations within or adjacent to KTH.

Data security

KTH shall conduct systematic, ongoing, risk-based data security activities supported by a management system. This management system shall reflect the needs of the organisation and control all processing of data for which KTH is responsible. Data security operations shall be coordinated and conducted based on the organisation's direction, with regular evaluations and continuous development.

KTH shall classify data and identify, analyse and assess threats and risks associated with the organisation's data, systems and services, as well as take adequate measures to protect the data. KTH shall have procedures in place for identifying, reporting, assessing, managing and documenting incidents that may impact on the security of data processing for which KTH is responsible or that KTH is conducting on behalf of another organisation.