Universiteit Leiden

Information Security Statement

In this age of digitisation and chain integration, Leiden University attaches great importance to the quality and reliability of information. Information is one of our key operating assets in the domains of Research, Education, and Operational Management. The reason is that accessible and reliable information is essential for a university.

As a leading university, we wish to offer our students, researchers, staff members (including lecturers), and chain and other partners safe and reliable information services.

Our 'Strategic Policy on Information Security' is our guide in safeguarding adequate information security within Leiden University. Our vision on information security is based on our awareness of the growing threat of cybercrime and State actors, as well as our growing dependence on digital processes and systems. We recognise that successful teaching and research activities increasingly depend on well-protected information, new technologies, and computer systems.

Important objectives in our information security policy are ensuring the reliability and continuity of educational, research, and operational management processes, offering a safe learning, research, and work environment, and managing information security risks by taking suitable control measures.

We rely on five policy principles:

1. *Information security is risk-driven*
   We base our measures on the potential security risks of our information, processes, and IT facilities.

2. *Information security is everyone's responsibility*
   Everyone is and feels responsible for the correct and safe use of resources and powers. Policy and technical measures are not enough to exclude risks in the field of information security. People themselves form the greatest risk, which is why we work tirelessly to raise awareness of security in order to increase understanding of the risks and encourage safe and responsible behaviour.

3. *Information security is a continuous process*
   Information security is encoded in the DNA of all our work activities. Information security is a continuous process, in which we continuously look for potential improvements. We do so among other things with the help of annual plans, checks, and adjustments.

4. *Security by Design*
   From the start, information security has been an integral component of every project and meeting concerning information, processes, and IT facilities.

5. *Security by Default*
   Users only have access to the information and IT facilities they need for their work. Making information available is a conscious choice.

To guarantee the effectiveness of our information security policy, we carry out regular checks, assessments, and audits. In this context, we evaluate compliance with the policy and report on this to the Executive Board. The Chief Information Security Officer (CISO) also assesses the effectiveness of the information security management process on an annual basis, and advises the Executive Board on the basis of the collected data and information.

We invite you to read the full text of the 'Strategic Policy on Information Security', which describes our vision, objectives, guiding principles, and responsibilities. Together, we aim to create a safe, reliable, and future-proof Leiden University that guarantees the privacy and rights of our students, lecturers, researchers, staff members, and other stakeholders.

For any questions concerning this policy, please contact us at security@BB.leidenuniv.nl