Leiden University Security Statement

How Leiden University deals with security

Data concerning students, staff and professional contacts are recorded as part of the teaching and research process and of management activities. In the privacy statement we explain how the University handles personal information collected and used in the course of these processes. This security statement provides information on how Leiden University deals with information security.

Basic principles

The University takes security and privacy seriously and strives to ensure that user information is obtained and stored in a secure manner. This security statement aims to clarify the security measures in place so that you can be assured that your information is adequately protected.

Leiden University treats information security in accordance with the Information Security Code (NEN-ISO/IEC standard 27001/2). Personal information is processed in accordance with the Personal Information Protection Act.

The aforementioned standards are elaborated in a number of documents. Particularly important are the Information Security Policy and the Baseline of measures that must be taken. Systems are subjected to risk analyses in order to determine how information should be classified and subsequently determine the measures that need to be taken for those systems. Additionally, campaigns are conducted to increase awareness on the part of staff and students.

Information security

The goal of security is on the one hand to safeguard the continuity of operational processes and on the other to minimise possible damages, whether direct or indirect, arising from security incidents. This goal is attained by putting into place a balanced package of preventative measures (preventing incidents), as well as repressive and corrective measures (aimed at limiting the negative consequences of incidents). The Information Security Code addresses not only securing information in computers and networks, but all forms of information, including, for instance, information stored in paper documents.

Information security has three aspects: availability, integrity and confidentiality. The availability must correspond to how the information is used in the process, and the university therefore takes measures against such issues as computers that are overloaded or do not function properly. Integrity involves measures that prevent unauthorised addition, modification or deletion of information. Confidentiality is important so that the network is not accessed or compromised by hackers by some other means.

Security principles

A number of security principles that the university adheres to are:
- we provide all ICT facilities with logical access control (access only after explicit permission; all users are uniquely traceable to a real person; the user's authenticity is determined on the basis of identification)
- we divide ICT facilities into zones within which information can be freely exchanged. Exchanging information with other zones proceeds via interfaces, the purpose of which is to isolate risks.
- we use a variety of physical and logical security measures. This means that breaking through one measure will not lead to the collapse of the entire system.

Auditing

Because developments in information security move quickly, each year and whenever a system is modified, risk analyses and audits are conducted to determine whether the measures are still adequate. These audits are tested by an external party. The results of the audits serve as input for new measures.

In spite of all these efforts, it can still happen that an incident occurs. Processes have been put in place to deal with such incidents. Absolute security cannot be guaranteed. When Leiden University learns that its security has been compromised, we keep the affected users informed so that they can take protective measures. The compromise will also be remedied as quickly as possible. Notification procedures consist of either informing users by e-mail or publishing an announcement on our website.