Information security policy for teaching, research and business operations at Leiden University

Universiteit Leiden

Version management

Version 0.1	29 July 2013	1st draft
Version 0.2	5 August 2013	2nd draft after input from Jan-Willem Brock. As well as trends incorporated after discussion with Johan Detollenaere. Input from Erik Adriaens.
Version 0.3	20 August 2013	3rd draft after input from Jan-Willem Brock
Version 0.4	4 September 2013	4th draft after input from Maritta de Vries
Version 0.5	21 October 2013	5th draft after input from Erik Adriaens, Johan Detollenaere and Gerrit Vooijs
Version 0.6	4 November 2013	6th draft after input from Jan van der Boon
Version 0.7	20 November 2013	7th draft after input from Daniel Mandel, André Morsman, Peter Magielse, information managers and Rinke Betten.
Version 0.8	16 December 2013	Modified as result of OBV discussion
Version 1.0	11 February 2014	Final. Decided by the board (same as 0.8)

List of abbreviations

AIC: Audit and Internal Control

Baseline: document with (basic) information security measures

Business Continuity: measures for disasters

CERT team Computer Emergency Response Team (team from ISSC)

DDoS: Distributed Denial of Service attacks

FM: Functional Management

IM: The Information Management department

IS: Information security

ISO: International Standards Organisation

ISSC: ICT Shared Service Centre

LDE: The Leiden, Delft and Erasmus Rotterdam universities

LIACS: Leiden Institute of Advanced Computer Science

Malware: cover term for viruses, Trojans, spam, etc.

NCSC: National Cyber Security Centre

NEN: Dutch norms for standardisation

OBV: Consultation of the directors of Administration

PID: Project Initiation Documentation

RASCI: Responsible/Accountable/Sign Off/Consulted/Informed

R&O: Performance and Development Interview

SAP: Business management software

SURFibo: SURF’s information security council

ULCN: Leiden’s identity management system

Executive summary

Leiden University wants to actively contribute to the security and perceived security of all university students, researchers and staff and all of its guests. This is not due to a lack of security, but in order to ensure a secure environment. Security is a precondition for a good academic climate in which those involved can flourish. As a research institution the University also wants to contribute to the development and improvement of security of society.

Every day there are news reports of hackers who penetrate systems or who have used malware to extract data from systems and disclose it. Organisations where this occurs can have their image tarnished, and their continuity can be jeopardised. To prevent this, an up-to-date information security (IS) policy is important. Reliable information for teaching, research and business operations is of crucial importance for providing high-quality, efficient service to students, researchers and staff. It is also a precondition for successful collaboration with external partners.

In addition to teaching and business operations, research is a topic that receives extra attention in information security. Protecting data in systems is important to be able to carry out research tasks properly, as well as to be able to safeguard academic integrity.

The following basic principles apply with regard to our information security policy:

- Leiden University is an open institution. This openness characterises both its teaching and its research.
- To guarantee that individuals (employees, students, guests and external parties) do not put the university's continuity at risk—intentionally or otherwise—certain processes, procedures, guidelines and codes of conducts have been drawn up and implemented.
- The implementation of these measures can be either organisational or technical in nature.
- Information security is largely driven by imposed legislation, and although the objectives are subscribed to, it is often perceived as a burden. In addition to securing information, explanation and awareness are thus an important component.
- The baseline established in this policy applies to all information and information systems, whether under the university's own management or subcontracted.

An important component of information security is looking at the importance of the data in the information systems. The availability, reliability and integrity of a system or of research data is examined on the basis of a risk management analysis. By using a questionnaire, these issues are assigned a rating, and it is determined whether the risk to which a system or research data is subjected is normal (basic risk), increased or high. Extra measures are taken depending on the risk.

Contents

1. Introduction

1.1 General

Information security (IS) is a current topic. Every day there are news reports about things such as botnets, information being tapped into by (foreign) governments, DDoS attacks on banks, viruses that make charges to your bank account, spam, phishing and other sorts of malware. This clearly shows that more attention must be paid to these issues and that measures must be taken to counter these attacks.

Due to these developments, the Dutch cabinet has also seen cause to establish a National Cyber Security Centre, which has the task of increasing Dutch society's resilience in the digital realm by providing advice on how to better secure systems. Institutions like Leiden University are expected to incorporate this advice into their own policies.

Information security at Leiden University is not only a support process. Knowledge institutions also play a role in research on developments in the area of computers and software. Two examples are the LIACS, where research is conducted on algorithms for securing information, and the International Centre for Counter-Terrorism (ICCT) where cybersecurity is one of the focal points.

Just like many other organisations, Leiden University is increasingly dependent on information stored in systems, which are often automated.

This dependence entails new vulnerabilities and risks, which need to be curtailed with appropriate measures. This is because insufficient information security can lead to unacceptable risks when conducting the university's educational or research activities and business operations. Incidents and break-ins in these processes can lead to financial damages and damage to one's image. The Executive Board therefore wants to systematically address the issue of securing its information services.

The previous information security policy and the baseline derived from it (minimum measures) date from 2010 and are due for a revision. Revision is desirable because new trends and developments are constantly taking place that influence information security. Furthermore, the governance model has been expanded, and the policy concerning business continuity has been added.

The policy and the baseline of minimum measures have been drawn up under the responsibility of Information Management's department of Administration and Central Services, in close consultation with the information managers of the faculties, the security officer from ISSC and the security manager from Real Estate. This policy concerning information security is one of the four priorities in the ICT infrastructure and ICT services as formulated in the ICT multi-year plan for 2012–2015.

1.2 Trends

In this section a number of trends are discussed in the area of information security in relation to teaching, research and business operations.

1.2.1 Teaching

In teaching a number of trends can be observed, such as digital instruction and students bringing that own devices (‘Bring Your Own Device’).

Digital instruction for students is becoming more and more important. Class lectures are recorded live, and students can watch them at a later time. It is also possible to take courses at domestic and foreign universities using open courseware and through massive open online courses (MOOCs). Legislation covering this information depends on the country where this data is hosted or passes through and where the companies providing the services are located. The American Patriot Act is by far the best-known piece of legislation, but every country has laws that make it possible to request information that is the property of Leiden University. Having students from dozens of countries participate in “The law of the European Union” is something positive from a publicity perspective, but it is a risk as far as information security is concerned.

The way our own lecturers and students work and live is becoming increasingly digital, with an ever-greater diversity in terms of devices and applications (apps). It is not possible to check the hundreds of different device models or the millions of applications (apps) ahead of time.

1.2.2 Research

In research, industrial espionage and Big Data are significant developments for information security.

Industrial espionage has always been around, and acquiring intellectual property can give a country or organisation a head start in developing certain products. Leiden University offers education, but it also conducts research, in which the value of information plays a role. If this value is high, third parties have an interest in acquiring this information illegally. The question is then how this information should be protected. Should individuals from certain regions of the world be excluded?

Big Data can particularly be found in the university’s faculty of Mathematics and Natural Sciences. Managing and securing large quantities of data is another area of research in which the university is active in an academic capacity.

And finally, two trends are the shift in university funding from direct government funding to indirect funding and beyond and the increasing importance of valorisation. Whereas with teaching the principle of “open by default” prevails, the situation is perhaps the opposite with research, especially with valorisation.

1.2.3 Business operations

One of the trends in business operations is working independent of time, place and device (currently also known as ‘The New Way of Working’). This can be working at home, but can alternatively be at some other location independent of the workplace. Furthermore, increasing use is being made of mobile devices such as tablets, smartphones and laptops. With these forms of consumerisation, the location where the data is stored plays a role—on the device or at the workplace—as does how this data is secured.

Trends in computer crime include increased usage of phishing, botnets and malware. Phishing in the Netherlands targets the bank sector as well as other sectors. The end user’s computer becomes infected—through a file in an e-mail message or when a certain website is visited—with a programme that lodges itself in the web browser. Once the computer is infected the attack can begin. In the case of a bank, the criminal can intercept the stream of communication between the client and the bank and modify the transaction.

Last year, botnets were once again an important tool for Internet criminals. Huge numbers of computers fell under the control of criminals when personal computers became infected by clicking on e-mail attachments. Botnets are used to send spam, conduct phishing or steal credit card information. Additionally, identity information is being bought and sold, and botnets are offered for hire. A great deal of transactions on the underground market are paid for using stolen credit card data.

In additional to the aforementioned methods, viruses and other sorts of malware are a significant issue. The attacks are becoming more and more sophisticated. Not only do attackers use attacks targeting a specific victim based on a lot of personal information (ransomware), but they also misuse websites that attract large numbers of visitors, such as newspaper websites, so as to infect as many computers as possible.

In the past few years more attention has been paid to privacy on the Internet. Social media platforms like Facebook and Twitter have had a particularly tough time because they are retaining and storing increasing quantities of user data, resulting in an increase in the associated risks. They also share data with third parties. Users become aware of this and become more critical.

With Hacktivism, computers and networks are used to attain an ideological or political goal. This is usually done by damaging opponents’ websites or making them unavailable.

1.2.4 Analysing the threats

As was shown in the above trends, threats are evolving at an ever-faster rate. Consider, for example, acts by extremists, DDoS attacks on systems, as well as non-ICT threats, such as cracking safes in order to scan exams or tests before they are given. In this context, Leiden University's increasing growth and the complexity that this entails requires a combined inventory and analysis of possible threats. This inventory was conducted in 2013 with the faculty directors of administration, the managers of the centres of expertise, University Libraries and Administration and Central Services. The following top risks emerged from that inventory: various forms of hacking, power cuts, DDoS attacks, espionage, damage to reputation for teaching, research and integrity. Other risks were student associations, water damage and leaked information. Measures will be provided in the baseline for the ICT threats posed by these risks.

1.3 Relation between information security and the protection of personal information

Data protection aims at dealing with personal data carefully. This means the data of students, staff and guests. The measures that are taken as part of information security contribute to the protection of sensitive personal data.

Within Leiden University the security manager is responsible for coordinating all activities related to information security. The data protection officer monitors the rules for data protection, and this task is assigned to the Legal Affairs department.

1.4 Relation between information security, physical security and occupational health and safety

Integrated security is an approach to gain control of all incidents and security risks in an organisation. These are brought in relation to each other, and appropriate measures are taken to counter or reduce the risks. Integrated security uses shared processes to create an overall picture of the security situation, regardless of whether there are occupational health, safety, security or IT risks. Integrated security improves the management and control of all security functions and results in a competitive advantage.

In Leiden there is increasing collaboration between the domains of information, real estate and occupational health and safety. An example of this is the policy regarding Business Continuity Management. Disaster plans are being drawn up for the entire university containing these various components.

1.5 The objective of information security policy

The goal of the information security policy is to safeguard the continuity of the information systems and to minimise damage by preventing security incidents and minimising possible consequences.

Among the elements provided by the information security policy is a framework in which (future) measures in information security can be tested against an established best practice or standard. For the standard the policy is based on the Information Security Code. This code is an NEN standard and describes standards and measures that are important for achieving an adequate level of information security. Attention is paid given to the legal requirements that must be taken into consideration. Organisational embedding is achieved through the description of the governance.

1.6 Scope of the policy

The information security policy concerns all individuals (internal and external employees, students, guests, visitors and business contacts), procedures and processes, and information and information systems (whether managed by the university or subcontracted). Information systems includes the basic infrastructure (including other networks, workplaces and storage), concern systems (institution-wide systems) and the specific systems of faculties and units. Mobile devices are also covered by the policy. An information security policy guide has been put together in which specific measures are listed.

There is an important relation and a partial overlap with related policy areas such as safe (occupational and environmental legislation), security (physical security) and business continuity. In all these areas, due attention is given to these overlapping areas and coordination is sought in terms of both planning and content.

The information security policy concerns both verified information, which is generated and managed by the institution itself, and unverified information (statements made by students in discussions, personal websites on commercial personal pages) for which the institution may be liable.

1.7 Responsibility for information security policy

It is the Executive Board that is ultimately responsible for the information security policy and which has decided on this policy. The security manager is responsible for maintaining the policy. Information security is a shared responsibility, whereby the owner of the information or system is responsible for applying the policy. The responsibilities are further elaborated in section 5.

1.8 Supporting documentation

This information security policy is further elaborated in a number of documents:

1. The baseline of minimum measures that systems must meet
2. Risk analysis document for determining risks and measures
3. The code of conduct for students and employees at the university
4. Guidelines and procedures
5. Guidelines, with translation into products and services

1.9 Contents of information security policy

The basic assumptions and principles of the policy are set out in section 2. Legislation and regulations are discussed in section 3. Section 4 describes business continuity. Section 5 discusses how information security is organised, and finally, section 6 describes how incidents are dealt with.

2. Vision, ambition, basic policy assumptions and policy principles

2.1 Outlook

As a socially engaged institution, Leiden University closely follows changes in the world and in the immediate vicinity of university, not only from the perspective of its core activities—teaching and research—but also in light of the significance of these developments for the organisation and its core values. Social and technological developments directly influence the university's situation. New developments offer opportunities for exploration, as well as risks. The open character of the institution makes it a mirror of society. For that reason the university as an organisation is not immune to changes in risks and perceived risks.

The challenges of modern society just sketched, such as globalisation, technological advances and individualisation, as well as the changed way of thinking about security, can have a negative influence on some of our core values, such as "open" and "personal", as well as on concrete organisational goals such as the desire to provide a "vibrant and secure campus". By and large, the degree to which society accepts risks—and especially security risks—is on the decline. With a government whose role is diminishing, organisations are more dependent on themselves than before. They will need to take their own measures to prevent risks and manage crises. They are even being actively called upon to do so. The environment is also setting ever higher requirements for the level and quality of our security and our ability to solve our own problems.

Leiden University wants to actively contribute to the security and perceived security of all university employees and students and of all of its guests. Not due to a lack of security, but in order to continue ensuring a secure environment. Security is a precondition for a good academic climate in which those involved can flourish without hindrance. As a research institution the university also wants to contribute to the development and improvement of the security of society.

2.2 Ambition

"We want to safeguard the information security of students, staff and guests by further strengthening the measures in place in order to be able to continue guaranteeing the integrity of teaching and research in the future and ensure that incidents remain limited and that their consequences are kept to a minimum."

The aim is to maintain the current level of security and to increase it where that is possible. This is no easy task. Social developments, as described in the subsection in section 1 concerning trends, pose new challenges for the university. Furthermore, the university must satisfy current laws and regulations, which in the area of information security are growing. But where needed, we also want to be able to make our own choices that suit our ambitions.

2.3 Characteristics of the organisation that influence the security situation

The following characteristics influence our security situation:

- The open character of the university as an educational institution
- The large number and diversity of its employees, students and guests
- The digitisation of information
- The importance of academic freedom and autonomy
- Working independently of time, place and device
- The increasing use of mobile devices (tablets, smartphones, etc.)
- Declining privacy awareness (information on Facebook)
- Intellectual property is becoming more and more interesting, enticing countries to engage in industrial espionage
- Due to research (for external parties), the amount of confidential data is increasing (closed character).

Because a number of the aforementioned characteristics can lead to more information becoming public than desired, it is important that the data be secured and that users' awareness be heightened. This policy includes a number of policy assumptions and policy principles to that end.

2.4 Policy assumptions

Security management is set up as a continual process. That entails that the annual planning and monitoring cycles are taken as starting points. It is within these cycles that annual plans are drawn up and implemented. The results are evaluated and translated into new annual plans.

The policy assumptions are:

- Leiden University is an open institution. Both its teaching and its research are characterised by this openness.
- To guarantee that individuals (employees, students, guests and external parties) put the university's continuity at risk—whether intentionally or otherwise—certain processes, procedures, guidelines and codes of conducts have been drawn up and implemented.
- The implementation of these measures can be either organisational or technical in nature.
- Information security is largely driven by legislation that has been imposed, and although the objectives are subscribed to, it is often perceived as a burden. Besides securing information, explanation and awareness are thus an important component.
- The baseline established in this policy applies to all information and information systems, whether under the university's own management or subcontracted. No compensation is made for information and information systems that have a lower

security level (shared burdens). The supplementary measures of a higher order are the responsibility of the system owner.

- For employees, at the time of hiring, during employment and upon termination of employment, the supervisor will inform the employee of his rights and duties for information security. For students and researchers, they will be informed of these rights and duties at the beginning of their study programme or work. When it is found that an individual (student, researcher, employee, guest)—consciously or otherwise—fails to comply with the information security policy, one is obliged to bring up the matter with him and report that according to an established procedure.
- If the IS policy is violated, the Executive Board can impose a sanction.
- All faculties and units have taken adequate measures (technical, procedural and organisational) for the individuals, information and information systems for which they are responsible to safeguard the continuity of business operations. They have designated an employee—the information manager/security officer—who enforces the policy and reports on compliance with the policy and on security incidents. It is the management of the faculty or unit who is ultimately responsible for introducing and implementing the IS policy within its unit and who is liable for damages resulting from correct or incorrect compliance with the IS policy.
- Security should safeguard the following aspects:
    - Availability (the degree to which data or functionality is available for users at the appropriate times)
    - Integrity (the degree to which data or functionality are correctly input or not damaged)
    - Confidentiality (the degree to which access to data or functionality is limited to those who are authorised)
    - The basic level of security has been translated into the measures as listed in the baseline (minimum measures).

2.5 Policy principles

The policy principles are:

- Information regarding the primary processes and business operation is open where possible and closed where necessary.
- Confidential information will be dealt with in a responsible manner**.**
- Information security is a line responsibility.
- Security management is set up as an institution-wide process. The yearly planning and monitoring cycle (plan, do, check, act) is based on ISO 27001**.**
- The university is the owner of information that is produced under its responsibility and is consequently responsible for its security**.**
- With (ICT) projects concerning primary processes and business operations, (information) security will be taken into account from the beginning. Each Action Plan includes a passage on the consequences for (information) security**.**
- Technical security is end-to-end and based on multiple strategies. These security measures will allow the university to react quickly to cyber ttacks and the like. Moving from analysis and classifying threats to protection and stopping them can be seamless.
- Within each business process there are risks in the area of availability, integrity and/or confidentiality. Only if these risks are clear can the management make choices regarding the implementation of measures that sufficiently lower the residual risk for the institution.

A few of the above-mentioned principles will now be explained in greater detail.

2.5.1 Information security is a line responsibility

The university's IS policy provides the framework. System owners and directors designated by the faculty management are expected to work the policy out in further detail. This is because they are the ones responsible for the correct implementation of the business processes assigned to them, along with the associated information services and for their proper functioning, and therefore also for information security. They have risk analyses conducted, from which measures can be derived to be implemented by ISSC and other parties. They continue to bear the primary responsibility for the selection, implementation and enforcement of these measures.

2.5.2 Expectations with respect to individuals

Leiden University is an open community that functions on the basis of trust. Everyone who works or studies in the community is expected to make efforts to ensure security both in his/her own interest and that of the university. It is everyone's job to deal with confidential information in a responsible manner. This includes both confidential information that is received and must not be divulged at all and confidential information that should not be divulged carelessly.

Security is an integral part of normal activities, a qualitative aspect that must be taken into account in all activities. This implies that it must be made clear what security tasks constitute an integral part of the set of tasks performed in individual positions.

2.5.3 Information security is a continuous process

To give information security adequate shape, a coherent package of security measures needs to be drawn up and maintained. This is a process that begins by specifying the security requirements and preconditions upon which the policy will be built and by setting up the organisation responsible for information security. Then it is determined what threats lead to unacceptable risks and what measures can be used to reduce these risks. On the basis of this information a package of measures is selected and then implemented. After the measures are implemented by the system owner, compliance must be monitored. Furthermore, it must be evaluated whether the package of measures implemented continues to meet the security requirements and preconditions and whether the relevant risks are being sufficiently reduced.

The security manager conducts regular reassessments of policy and monitors on the basis of risk analyses and audits. Technological and organisational developments inside and outside the institution make it necessary to periodically look at whether we are going about safeguarding information security in the right way. Audits of concern systems (institution-wide systems) make it possible to check both the policy and the measures taken for efficiency (verifiability).

The IS policy and the minimum measures are evaluated at least every four years for content, feasibility and implementation status and revised. The IS policy also makes provisions for audits and periodic risk analyses for systems.

Risk analyses are conducted by the security manager—under the ultimate responsibility of the system owner—when a system is first delivered and whenever it undergoes major modifications. With risk analyses it is assured that:

- the desired level of information security is laid out in the form of a data classification with regards to business processes.
- Measures are established keeping to the level of security determined.
- If any changes take place in the context, these are evaluated annually and the level and the measures are revised if necessary.

With respect to auditing, the IM department cooperates on the audits under the responsibility of the AIC audit department. Various audits are conducted each year on (concern) systems.

2.5.4 Ownership of information

As a legal entity, Leiden University is the owner of all information that is produced under its responsibility. Additionally, the University manages a large amount of information, or access thereto, which is the property of third parties (copyright). An example of this is the online content of journals that can be accessed through the Digital Library. It is incumbent upon the University to ensure that the security of this information is properly arranged for and that all its employees and students are adequately informed about regulations concerning the (re)use of this information.

2.5.5 Valuing information

Security takes place with a clear picture in mind of the value of what is being secured. That implies that awareness of the value and of the risks of possible damage is the foundation of the policy and must play a guiding role in taking measures. It is the task of the manager or director responsible in each faculty and unit to ensure that this awareness is present.

All information has an owner. The value of the information is determined by the owner. The value is determined by the damage that loss of availability, integrity and confidentiality causes for the ability to provide teaching and research at a high academic standard.

2.5.6 Projects and information security

With projects, such as modifications to infrastructure or the purchase of new systems, information security is taken into account from the beginning.

2.6 Classifying data and systems

All data in systems to which this information security policy is applicable gets classified. The level of the security measures depends on the category to which it is assigned.

The classification of information depends on the data in information systems and is determined on the basis of risk analyses. In this regard the following aspects are significant:

a. availability
b. integrity
c. confidentiality

Availability is the degree to which data or functionality is available for users at the appropriate times.
Integrity is the degree to which data or functionality are correctly input.
Confidentiality the degree to which access to data or functionality is limited to those who are authorised.

Aspects and characteristics of information security and related threats:

Aspect	Characteristic	Threat	Examples of threat
Availability	Timeliness	Delay	Infrastructure overload
	Continuity	Outage	Faulty infrastructure
Integrity	Correctness	Modification	Unauthorised changes to data; virus infection; typographical error
	Completeness	Removal	Unauthorised deletion of data
		Addition	Unauthorised addition of data
	Validity	Obsolescence	Failure to keep data up to date
	Authenticity	Falsification	Fraudulent transaction
	Irrefutability	Denial	Denying having sent a particular message
Confidentiality	Exclusivity	Disclosure	Listening in on the network; hacking
		Misuse	Large-scale private use

2.6.1 Classifying data in concern systems

What security is appropriate for a particular information system depends on how the information processed by the system is classified. The classification must be determined by or on behalf of the owner of the information system in question. This is done with the help of damage scenarios.

The following are the damage scenarios concerned:

- damage to the (main) business process
- direct financial damage
- (breach of) agreements
- damage to reputation
- personal injury
- (violation of) laws and regulations

In each of these damage scenarios the information security aspects of availability, confidentiality and integrity are examined, as is the question of whether the impact is low, medium or high.

For each of these qualitative aspects there is a structured questionnaire. On the basis of the answers to these questions, a risk analysis is periodically drawn up for each system. The analysis leads to each system being assigned to a risk category: (see below): basic (normal) risk, increased risk (sensitive) and high risk (critical).

The table below shows what security level corresponds to what category of information.

Risk category	Description	Measure	Systems
Basic risk (level 3)	Breach in availability, exclusivity and integrity does not cause a (major) disruption.	The system must meet the minimum measures (IS baseline)	Planon, Converis
Increased risk (level 2)	Breach in availability, exclusivity and integrity does not cause a disruption of serious nature	The system must meet the minimum measures and extra measures	SAP, Blackboard, Docman
High risk (level 1)	Breach in availability, exclusivity and integrity cause a disruption of serious nature, putting the continuation of primary processes at risk.	The system must meet the minimum measures and extra (heavy) measures.	ULCN, uSis, (Web CMS), network systems

The baseline level is the level of basic risk. This means that a risk classification has been carried out and the availability, confidentiality and integrity on that level are low. For this level, measures have been drawn up which every system must meet. If the system has an increased or high risks, extra measures must be taken.

2.6.2 Classifying data in systems for research

In principle, the classification of data in a system used for research is conducted in the same way as that of data in concern systems.

The following damage scenarios are concerned:

- damage to the (main) business process
- direct financial damage
- (breach of) agreements
- damage to one’s image
- personal injury
- (violation of) laws and regulations

In each of these damage scenarios the information security aspects of availability, confidentiality and integrity are examined, as is the question of whether the impact is low, medium or high. The data in the system is ultimately assigned to one of the risk categories, and the measures must be adapted accordingly.

The procedure is different in the sense that with concern systems it is the security manager or security officer of the ISSC who conducts the risk analysis, while with systems for research this is done by the information manager/security officer of relevant faculty.

With research having a high risk profile the faculty information manager/security officer will conduct a risk analysis together with the person responsible for the research. The security manager provides the information manager with a methodology for conducting the analysis. After assignment to a risk category, measures must be taken, using the baseline as a guide.

2.6.3 Confidential data in paper documents

For data in confidential (paper) documents, it is determined beforehand who shall have access to these documents and how the data will be provided physically. After use, the files are immediately put away in a locked cabinet. If another—unauthorised—employee needs to examine confidential documents, this needs to take place under the supervision of the manager responsible.

2.7 Audits

Audits on systems take place according to the audit calendar. The frequency is determined on the basis of how the system is classified. The audit is conducted during the project phase and gives a picture of the system’s vulnerability and dependence. All concern systems are in the audit calendar. (Concern systems are systems that support university-wide processes.) The frameworks of standards against which these are tests are SURF (based on the Code for Information Security) and KPMG (SAP and uSis). The two frameworks have the same sources, and it would be desirable to eventually replace them with a single framework of standards.

3. Laws and regulations

The university information security policy is subject to laws and regulations. Additionally, internal guidelines and codes of conduct have been established for everyone who works or studies at Leiden University or who uses the university’s information services. These legal requirements and internal regulations will now be briefly discussed.

3.1 Legal requirements

General legal requirements must be complied with. This is especially relevant for:

- Higher Education and Research Act
- Personal Information Protection Act
- Archive Act
- Copyright Act
- Telecommunications Act
- Computer Crime Act

Higher Education and Research Act

Leiden University has a quality assurance system, which safeguards the careful handling of data in the student administration and with academic performance information (among other things). Codes of integrity for scholarly research are also complied with and applied.

Personal Information Protection Act

The Personal Information Protection act sets requirements for the storage and processing of personal information, particularly for the correctness and accuracy of personal information, as well as requirements for conducting appropriate technical and organisational measures to secure personal information against loss and unlawful use. Compliance with this information security policy and implementation of the minimum measures should result in compliance with the Personal Information Act.

Archive Act

Leiden University follows the requirements in the Archive Act and the Archive Decision concerning the way information should be handled that is recorded in—digitised—documents, information systems, websites and the like.

Copyright Act

The Copyright Act governs the copyright of original works in the areas of literature, scholarship and art. This means that the University does not distribute original works without obtaining permission from the copyright owner. It also means that efforts are made to combat the use of illegal software.

Telecommunications Act

The Telecommunications Act governs all sorts of matters relating to the flow of information over public networks. As long as the network is not public, the Telecommunications Act is not applicable.

Computer Crime Act

The Computer Crime Act concerns problem areas in criminal law related to the use of computers. The Computer Crime Act stipulates that “some security” is required before there can be any possibility of criminal proceedings for offences against the university and of the indemnification of university managers.

The law includes specific penalties regarding issues such as:

- penetrating a secured computer system (computer-based disruption of the peace)
- the illegal modification and addition or data on a computer, even if the data is not secured;
- damaging, rendering unusable or disruption of a computer system, whether intentionally or due to negligence

Obligation to report data leaks

The Personal Information Protection Act is expected to be amended in 2013 in order to introduce an obligation to report the breaches of measures for securing personal information (obligation to report data leaks).

A security error can result in large amounts of personal information becoming public. The oversight body—the Personal Information Protection Board (CBP)—receives notification. In many cases the person whose personal information is concerned is also receives notification, if the break-in is likely to have negative consequences for his or her personal life circumstances.

This means that, in the case of a data leak, Leiden University's incident response team will report the leak to the CBP and immediately indicate what the consequences are and what measures have been taken to remedy these consequences. The ISSC has put procedures into place for this obligation to report.

3.2 Other guidelines and nationwide agreements

A portion of the university guidelines has been drawn up in consultation with SURF. The principal documents and guidelines are:

General guidelines:

1. Code for Information Security (NEN-ISO/IEC 27001/27002)
2. "Risk analyses for information systems" guidelines

University guidelines:

3. Codes of conduct for students and staff: such as acceptable use of information services, Student Statute
4. codes of integrity for scholarly research
5. The password policy
6. The identity management policy (ULCN)

SURF-IBO and SURFnet guidelines:

7. SURF-IBO guidelines pertaining to information security
8. Applicable Best Practices from SURF-IBO
9. SURFnet conditions for connecting the University to SURFnet
10. Surf Federation agreements

Other guidelines:

11. Studielink agreements

4. Business Continuity

4.1 Definition

Just like insurance, business continuity aims to identify potential threats, the impact they would have on the organisation should they occur (damage) and the cost of measures to prevent that. In the literature, business continuity concerns surviving a crisis or disaster. Further below in this memorandum business continuity is also discussed in relation to less serious threats (or incidents).

An example: there is a risk that a fire could erupt in the Snellius Building and that the ULCN system be destroyed. The impact of this incident is that users' passwords could no longer be verified and that users could not be able to access their documents, e-mail and business applications. This situation prevails until new hardware is found (purchased?), is put into place in another building and the back-ups are reinstalled (several days). The damage from this disaster is determined using loss in productivity and damage to the university's image. Measures can be pragmatic and cheap, such as using USB sticks to store documents without a password, or running a duplicate ULCN system in parallel at another location.

If more than one system suffers an outage, then it must be determined in what order the systems should be restored. Using the outsourcing strategy, the risk can be spread out somewhat. But this also results in extra complexity: due to the fact that different systems work in a chain, a subcontracted available service (such as Blackboard) could be inaccessible because some internal service (ULCN) is not available. Sufficient insight into these sorts of interdependencies is a precondition for a good business continuity strategy.

4.2 Policy

For existing services Leiden University has chosen not to take out insurance against crises in the area of ICT. This applies both to internal (shared) services with ISSC and the subcontracted management of Blackboard, uSis and SAP. For ISSC, in case of a disaster, steps towards restoration should be carried out as quickly as possible using the professional skills of ICT staff. In this connection the priority will be determined by specialists on the basis of the people and means available (hardware, back-ups and descriptions).

With decisions concerning contracts, new systems and major updates, a scenario based on guaranteed restoration within one week will be provided, so that the Executive Board can make explicit considerations basis on the costs.

4.3 Measures

The university has conducted significant preparatory work for the preconditions that pertain to the current strategy of not being insured, but the situation can still not be described as “in control”. At the level of central and decentralised management, training sessions and workshops are held for crisis management. For uSis, Blackboard and SAP, the issue concerning disasters is a component of the contract agreements and can be modified upon either renegotiation or a new subcontract.

Fortunately, disasters are an infrequent occurrence, making agreements concerning the level of service (so-called service level agreements) at least as important. Service level agreements target normal disruptions (incidents), and disasters are practically always excluded from the guarantees. The service levels of the various systems and components of the ICT infrastructure have still not been sufficiently examined in this connection. In this context, the fact that Blackboard is 99.7% available is of little benefit to the user if either the network or ULCN has a much lower availability.

5. IS policy governance

The term governance concerns running an organisation properly, efficiently and responsibly. It encompasses the processes, consultations, tasks and responsibilities of the interested parties, such as the owners, employees, students, other customers and society as a whole.

Information security governance is described in this section. It is important that the tasks, responsibilities and authorities pertaining to this area of policy are assigned unambiguously. This designation process aims to prevent things from being carried out redundantly or security tasks from being overlooked.

5.1 IS governance

This section describes how information security governance is organised and who is responsible for it.

	Exec	Security manager IM	Security Officer ISSC	IMer’s units / fac. Security off.	VG security manager	AIC head	IM head	Legal	FM heads	System owner
Policy development										
– IS outlook	A	R	C	C	C	C	S	I	I	I
– threat analysis	I	C	C	C	R	I	C	C	C	C
– classification of concern information – systems	I	R	C	C	C	S	I	C	C	A
– classification of faculty systems		I	C	R	I	I	S	I		
– draw up and maintain ICT chapter in integrated crisis management plan	A	C	C	I	R	I	S	I	I	I
– draw up and maintain prioritisation of information systems	I	R	C	C	I	I	A	I	C	C
– draw up and maintain prioritisation of information systems		C	I	I	I	I	I	R	I	I
– draw up and maintain code of conduct	I	R	C	I	I	I	A	C	I	I
draw up baseline	I	R	C	C	C	C	A	I	I	I

	Exec	Security manager IM	Security Officer ISSC	IMer's units / fac. Security off.	VG security manager	AIC head	IM head	Legal	FM heads	System owner
Advise on IS policy										
– Advise on projects		R	C	C	C		S	C	C	A
– Advise on units		C	C	R	C		I	C	I	I
– answer fac. information managers' questions		R	C	I	C		A	C	I	I
risk analysis of system		R	C	C	I	I	I	I	C	A
Management										
– coordinate major IS incidents and disasters	I	C	C	I	C	I	S	I	R	A
– coordinate minor IS incidents		I	R	I			S		C	A
- evaluate major IS incidents	I	R	C	I	I		A	I	C	C
– coordinate university-wide IS processes		R	C	I	C	I	A	I	C	I
Auditing										
– ICT auditing calendar	A	R	C	I	I	C	S	I	C	C
– conduct audits	I	R	C	C	I	A	I	I	C	C
– conduct risk analysis		R	C	C	I	I	A	I	C	C
– monitor following of recommendations	I	C	C	C	C	I	C	I	R	A

Table 1: Governance

Legend
R = responsible = responsible for implementation
A = accountable = ultimately responsible

S = sign-off = responsible for process

C = consulted = consulted during process I =
informed = informed of results

5.2 Organisation of the information security function

In order to handle information security in a structured and coordinated manner, tasks, authorities and responsibilities are assigned. In this section the organisation of the information security function is discussed. Due to the separate description of the information security function in this section, one might get the impression that an independent organisation needs to be set up for this. That is not the case. It is a matter of assigning tasks, authorities and responsibilities to officers within the existing organisational structure. For most security officers who engage in information security this topic will not be a full-time job, but will rather make up a portion of their job activities.

Executive Board

The Executive Board is ultimately responsible for information security within the university and establishes the policy and minimum measures in the area of information security. The responsibility for the substance of the information security is mandated to the head of the Information Management department by the director of Operational Management of Administration and Central Services The officer puts the security manager in charge of the task of conducting information security according to this policy (or having it conducted).

System owner

The system owner is responsible for seeing to it that the application and the information put into it provides proper support for the process for which it is responsible. This implies that the system owner ensures that the application continues to satisfy the requirements and desires of users and of laws and regulations, both now and in the future. Of course, the application must comply with the information security policy and at least with the minimum measures.

If a risk analysis makes it apparent that there is an increased or high risk, then additional measures are necessary. However, the system owner can deviate from these, provided that reasons are given and that the security manager is informed. The security manager examines the situation and makes the decision. He will advise the director of Administration and Central Services and the Executive Board about the risks that arise as a consequence.

Information security portfolio

Every faculty and unit, including the University as a whole, has a person in charge of the information security portfolio at the highest administrative level. This director is mandated by the management or unit to introduce and implement the IS policy within his faculty of unit. Within the Executive Board the person in charge of the business operations portfolio is also responsible for information security.

Security Manage (at Administration and Central Services/IM)

The security manager oversees compliance with the IS policy and resulting measures across the organisation, organises studies and advises on complex security issues, initiates risk analyses and security audits, organises business-wide security awareness programmes and fulfils an advisory role for the administration and management.

This role has a strategic character and is given concrete form by Administration and Central Services' department of Information Management. The security manager reports through the head of information management to the director of Administration from Administration and Central Services and to the Executive Board.

Security Officers (faculties and units)

The security office is the contact person within his faculty or unit for questions concerning information security. In faculties, in practice this will usually be the information manager. He/she is responsible for the implementation of and compliance with the information security policy and the minimum measures for systems of which the faculty concerned has ownership. This can entail conducting risk analysis for information systems (or having them conducted), drawing up information security reports and ensuring increased awareness.

Additionally, the security office identifies incidents and advises on how to resolve them. He/she is also the contact person for his/her own organisation for any internal and external contacts. Security officer is a role in which the officer reports to the person in charge of the information security portfolio within his own organisation.

The security office of the ISSC has a number of additional tasks. The security officer conducts risk analyses on the (concern) systems together with the security manager. The security manager is also informed if the minimum measures of the operational (concern) systems are not complied with, and he translates these into risks for ISSC services. The ISSC security office is also the chair of the CERT team, which either handles security incidents or redirects them to the relevant security officers in the faculties or the centres of expertise. Finally, the security officer is also the site security contact for requests from SURFnet.

Real Estate security manager

Real Estate's security manager has his own policy and measures pertaining to physical security. He is also responsible for drawing up and maintaining the crisis management plan and for coordinating major IS incidents and disasters. He is additionally responsible for the threat analysis and is informed and consulted for portions of the IS portions of IS policy development, management and auditing.

Head of AIC

The head of the Audit and Internal Control is responsible for monitoring, testing and evaluating the quality of administrative records and for the implementation of financial/economic policy, by means of audits for specific issues. Finances, business operations and automation are audited under his direction as part of the annual inspection of the books. These last audits are conducted on SAP and uSis by the security manager. SURF is audited as well.

Head of IM

The Information Management department's ICT policy section is responsible for the university's information policy. Each year an ICT project calendar is drawn up in which the CIT multi-year plan is translated into concrete ICT projects. One of the tasks of the department is information security. The security manager carries out his tasks under the direction of the head of IM. For all of the security manager's tasks in the governance IS model, the head is either informed and consulted or he/she is responsible for the process.

Head of Legal Affairs

The head of Legal Affairs and the security manager have activities that overlap, especially in the area of privacy and of writing and maintaining the code of conduct for the use of information services and equipment. Legal Affairs is responsible for privacy policy, while the security manager is responsible for the code of conduct. Legal Affairs is entrusted with the role of the data protection officer.

Heads of Functional Management

The heads of functional management are responsible for the functional management of systems such as SAP, uSis and other (concern) systems. Risk analyses or audits on systems shall be conducted with cooperation of these department heads. They will eventually discuss the results of these audits with the system owners, and they are also responsible for implementation of the accepted recommendations.

5.3 Coordination with overlapping policy areas

A part of the governance is that due attention should be given to all sorts of risks and their interrelations. It is for this reason that consideration is given to information security, as well as to physical security, occupational health and safety and business continuity. After all, it is a necessary requirement for governance that these disciplines work together.

This is made concrete by having the planning cycles for these domains run in parallel. That provides opportunities for noticing and addressing any interference between them. Where desirable and possible, this coordination is also translated into the tactical and operational level, but only where that would result in added value.

5.4 Awareness

Many users and managers of information are unaware of the risks to which one is exposed in the context of information security, or they are not sufficiently aware of the responsibility they bear regarding the information to which they have access.

Unfortunately, this makes for a fertile breeding ground for incidents. Research indicates that the cause of most security incidents can be found within the organisation itself. That is why awareness, or rather raising awareness, is an important instrument when it comes to information security. The security manager is responsible for the awareness raising process and develops a campaign on the subject on a yearly basis.

5.5 Monitoring and compliance

The implementation of information security is evaluated annually. This is done in the autumn as part of the inspection of the books and is coordinated with the normal planning and control cycle to the greatest extent possible.

Additionally, a SURF audit is conducted every two years under the direction of SURF-IBO. The framework for the evaluation is based on the Code for Information Security of the Netherlands Standards Institute. The issues listed in the Code constitute the starting point for evaluating the security situation at the university. The SURF audit consists of three parts: the information security policy, agreements, the registration and handling of incidents and the identity management policy.

5.6 Sanctions

When the rules pertaining to information security are violated, measures may be taken by or on behalf of the Executive Board. Measures could include, for instance, blocking access to the network or certain network services. In case of “spamming” (sending a very large number of undesired and unsollicited e-mails), the offender can be denied access to e-mail services.

A code of conduct is available for all users of Leiden’s information services, which is published on the university website (http://media.leidenuniv.nl/legacy/lei_gedragsregels_iv_nl_v3.pdf). This code is applicable to students and staff, as well as to third parties.

If it found that the rules of conduct have been violated, the Executive Board can impose a disciplinary sanction, as proposed by the person in charge of the information security portfolio at the faculty or unit where the violation occurred.

If Leiden University is contacted concerning violation of intellectual property rights or other regulations, or concerning the rights of others, Leiden University may charge the user who caused the damage for those damages. If damage is incurred due to misuse of computer and network services, Leiden University can charge this to the user who caused the damage.

6. Reporting and handling incidents

The management and registration of incidents pertains to the way that verified or suspected breaches of information security by employees shall be reported, as shall the way that these incidents are handled.

Each faculty and unit bears responsibility for identifying and reporting incidents involving and breaches of information security. Staff can report incidents pertaining to data or individuals to their faculty's security officer/information manager. The security officer can resolve the incident himself or with the help of others, after which time the incident can be cancelled.

Security incidents like phishing or spam can be reported to the CERT of the ISSC at abuse@leidenuniv.nl.

The Computer Emergency Response Team (CERT) focusses on the technical aspects of information security and is responsible for:

- Gathering information about potential ICT security incidents and security leaks
- Centrally registering ICT security incidents
- Analysing and evaluating the nature, extent and cause of the ICT security incident
- Organising the evaluation of the way the ICT security incident not extending beyond the university was handled. If this does happen, the security manager takes the lead.
- Advising the standing organisation on the preventive measures and steps for restoration to be taken in case of ICT security incidents with limited impact
- Advising the crisis team on the preventive measures and steps for restoration to be taken in case of ICT security incidents with major impact
- Inform and instruct those directly involved about the preventative measures and steps for restoration to be carried out
- Centrally inform users about ICT security incidents
- Coordinate the implementation of preventative measures and steps for restoration

The incidents that are recorded include the following:

- Inexplicable irregularities in system and application log files;
- Failure of an integrity check for an information system or source of information;
- Loss of a source of information;
- Unplanned outage of information systems for longer than five minutes which the security officer deems to be an incident
- (suspected) break into the system;
- (suspected) misuse of a system or data by a legitimate user;
- (suspected) major outbreak of a virus on the university network or local network; (possible) very threatening outbreak of a virus on the Internet.

The aforementioned incidents shall be registered and dealt with, and they must be used as input for incident reports.