University Information Management

UNIVERSITEIT TWENTE.

Reference: SB/UIM/15/0106/khv
Date: 7 December 2015

Status: Final
Date established by the Executive Board: 7-12-2015
Author: Wim Koolhoven

University of Twente Policy on Information Security

The University of Twente policy on information security has its basis in the Model Information Security Policy of Higher Education drafted by SURFibo[1] and published under the Creative Commons[2] licence.

Summary

Great importance is placed on the availability, integrity and confidentiality of the information provided. This policy establishes how these aspects are guaranteed at the University of Twente. The importance of information security is also reflected in the SURF report 'Cyber threat assessment'.[3]

The University of Twente complies with the law and therefore handles information about students and staff as carefully as possible. A proactive attitude on the part of each employee is crucial to this, however no more measures are taken than strictly necessary to avoid frustrating the University of Twente's entrepreneurial and creative nature.

Data security is everyone's responsibility and constitutes a line responsibility. Managers bear primary responsibility for properly securing data in their department/unit. All information systems are classified on the aspects Availability, Integrity and Reliability. This classification determines the level of security measures.

The responsibilities of all officials involved will be described, in particular those of the Security Officer, Security Manager, System Custodians and managers. The importance of regularly drawing attention to security risks and measures will be detailed further. The role of CERT-UT (Computer Emergency Response Team of the University of Twente) are laid down.

To create awareness and to influence the behaviour of staff and students regarding information security and privacy, a working group will be set up by University Information Management.

The appendices detail relevant legislation, provide an overview of the other policy documents and codes of conduct in the area of information security and formulate the security rules (operational guidelines).

[1] Information security officers and privacy officers employed in higher education confer in SCIPR (SURF Community for Information Security and PRivacy, previously SURFibo). The objective is to improve information security and privacy at universities of applied sciences and traditional universities. SCIPR does this through the development of policy and guidelines, for example.
[2] See www.creativecommons.org/licenses/by/3.0/nl/deed.en
[3] Cyber threat assessment report for Higher Education and Scientific Research Sector www.surf.nl/kennisbank/2014/rapport-cyberbedreigingsbeeld-sector-hoger-onderwijs-en-wetenschappelijk-onderzoek.html (only available in Dutch).

1 Introduction

Information security means that a cohesive set of measures is taken and maintained to safeguard the availability, integrity and reliability of the information provided. It also relates to how to verify the measures that were taken to guarantee these quality aspects.

Information security is a policy responsibility of the Executive Board of the University of Twente. Operational management, but also education and research are increasingly dependent on information and computer systems, which may be subject to vulnerabilities and risks. It is therefore important that effective measures are taken. After all, insufficient security of information could lead to unacceptable risks in education and research and in the institute's business operations. Incidents and breaches of these processes could lead to financial losses and have a negative impact on the university's reputation.

First and foremost this current policy document aims to fundamentally raise the University of Twente's information security to a higher level and maintain it at that higher level through governance, legislation and regulation, and secondly, this document aims to clearly describe and establish how to organize the university's security position and information security policy, including their interrelationship. At the University of Twente, more attention is being devoted to privacy as legislation becomes increasingly strict. A separate privacy policy will be drawn up at the end of 2015.

1.1 Scope of the policy

At the University of Twente, the protection of information is interpreted broadly. A close relationship and partial overlap exists with other policy areas such as safety (working conditions legislation and environmental legislation), physical security and business continuity. Integral security requires proper harmonization between these other policy areas.

The information security policy at the University of Twente concerns all staff, students, guests, visitors and external relations (hired/outsourced) as well as all organizational units. The information security policy also includes all devices that provide authorized access to the institute's network.

The Information Security Policy emphasizes the information and applications that fall under the University of Twente's responsibility.

1.2 Background

The current Information Security Policy is out of date and is insufficiently known and addressed in the organization. The University of Twente participated in the SURFaudit in 2012 and 2013. The result offered an insight into the university level of maturity in the area of information security and privacy protection. At the beginning of 2015, the Executive Board decided[4]to established the university's ambition at a minimum maturity level 3: Defined Process. The University of Twente is not yet at the desired level (partly at level 1 or 2). The main issues are lack of awareness and proper conduct.

The current security policies were developed over the course of 2007 and 2008 and established in 2009. At the end of 2013 an assessment was conducted by ICTS to check whether an update was necessary. The conclusion was that although managers were aware of the existence of the policies, they were not sufficiently familiar with the contents and did not check newly set-up service departments against the policies. A second conclusion was that the policies were not in line with ICTS' terminology and method of working.

[4] Ambition level SURFaudit, reference SB/UIM/14/0902/khv, see www.utwente.nl/uim/informatiebeveiliging/ambitieniveau-surfaudit.pdf (only available in Dutch)

1.3 Brief history

After Information Management was set up, a new Information Security Policy was set up in 2008 together with the University of Twente's 2008-2010 Information and IT plan. In 2011 the readability of this document was increased while its length was halved in accordance with a national model. Furthermore, a great number of policy documents on sub-topics have been established over the past years.

The SURF report 'Cyber threat assessment' [5] published at the end of 2014, provided education and research institutes an understanding of the main threats to cyber security and privacy. The report helps to put cyber security and privacy high on the internal agenda and provides recommendations for taking appropriate measures to keep the available information secure, reliable and accessible.

In the winter of 2014-2015, the Information Security Policy was evaluated and revised in collaboration with representatives from the faculties and ICTS. A considerable amount of time was invested in wording a concise set of basic rules that express what we, as the University of Twente, feel is truly important.

1.4 Reader's guide

The different sections of this policy document can be read independently of one another. It describes the standards that require implementation by the relevant responsible parties. All readers are recommended to read at least subsections 3.1 Basic rules and 3.2 Policy Principles of Section 3 Principles. Section 4 concerns Governance and explicitly states how the responsibilities for information security have been assigned at the University of Twente. The roles of Security Officer, Security Manager and CERT-UT (Computer Emergency Response Team) are laid down in this section.

The appendices detail relevant legislation and outline the security rules (operational guidelines). Relevant ICTS staff are closely involved in the assessment of and adjustments to these rather technical security rules. By appending these security rules, the link between the security rules and the policy is clear. The security rules have been worded in such a way that they can be understood by people without a technical background. As regards ICTS staff who are only interested in the impact on their own work, it may suffice to just read the relevant security rules.

[5] Cyber Threat Assessment Report for Higher Education and Scientific Research Sector www.surf.nl/kennisbank/2014/rapport-cyberbedreigingsbeeld-sector-hoger-onderwijs-en-wetenschappelijk-onderzoek.html (only available in Dutch).

2 Objective of the Information Security Policy

The objective of the University of Twente's Information Security Policy is to safeguard the continuity of operational management, education and research and to limit loss by preventing security incidents and mitigating any consequences.

The objectives of the University of Twente's Information Security Policy can be specified as follows:

- *Framework*: the policy offers a framework to assess current and future measures in information security against a set standard and to allocate the tasks, powers and responsibilities within the organization.
- *Standards*: the basis for the set-up of security management is ISO 27001.[6] Measures will be taken on the basis of 'best practices' in higher education and on the basis of the ISO 27002 standard[7].
- *Explicit*: the principles and organization of the information security positions have been established and are supported by the Executive Board and indirectly by the entire organization.
- *Decisive*: basis for clear choices in measures, active monitoring of policy rules and their implementation.
- *Compliance*: the policy offers a basis to comply with statutory provisions.

[6] In full: NEN-ISO/IEC 27001: Requirements of management systems for information security
[7] In full: NEN-ISO/IEC 27002: Code for information security

3 Principles of information security

3.1 Basic rules

General strategy documents, such as Vision2020, do not provide a sufficient basis for an Information Security Policy, or in other words, a basis on which to formulate a risk acceptance appropriate to the University of Twente. To prevent a lack of awareness of the policy and thus support for it across our organization, it is important that we clearly express what is important to us.

1. *As a public-law organization, the University of Twente abides by the law.* Many consider this to be self evident. Even though the University of Twente is an entrepreneurial university, it does not subscribe to the view that an organization's decision on whether or not to abide by the law should be based on a cost-benefit analysis. Having said that, of course, it should be pointed out that the university is not law enforcement either.
2. *Information about students and staff is handled as carefully as possible.* Prospective and current students must be able to rely on the university to handle their information as carefully as possible. Much of this information is related to students' courses of study. Exercising due caution in matters of privacy is one of the challenges we face, as a university.
3. *All University of Twente staff are expected to adopt a proactive attitude, particularly with regard to information security in all processes and activities.* There are many aspects to information security, which touches on virtually all processes and activities. Taking risks is part of the University of Twente's entrepreneurial spirit. Part of this involves exploring potential consequences in advance and taking steps to mitigate any unacceptable risks.
4. *The Information Security Policy in no way interferes with the University of Twente's entrepreneurial and creative nature.* All necessary security precautions must be taken, of course, even though some individuals may not be particularly happy about it, but only after the matter has been carefully considered. Proportionality is called for here. No radical or restrictive measures that are disproportionate to the actual risk reduction involved will be taken.

3.2 Policy principles

Security management will be organized as a process. That means that the annual planning and audit cycle is based on ISO 27001[8] (Plan, Do, Check, Act). The annual plans are drawn up and executed along these lines. The results are assessed and translated into new annual plans.

The following aspects of information must be ensured by the security:

- **A**vailability: the extent to which information or functionality is available to users at the right times and in the right locations;
- **I**ntegrity: the extent to which information or functionality has been correctly specified;
- **C**onfidentiality: the extent to which the access to information or functionality is limited to those who are authorized.

The University of Twente respects the following policy principles:

- Information security is **everyone**'s **responsibility.** Communicate to staff, students, lecturers and third parties that they are expected to contribute actively to the security of the computerized systems and the information stored in them. This could be communicated in, for example, the letter of appointment, during annual performance appraisals, with an institutional code of conduct, through periodic awareness campaigns, etc.

[8]In view of the fact that ICTS uses ITIL, using ITIL Security Management is appropriate for ICTS, as this is based on ISO 27001 and it develops the link with the other ITIL processes.

- Information security is a **line responsibility.** This means that managers bear primary responsibility for properly securing information in their department/unit. This also includes the choice of measures and their performance and enforcement.
- Information security is a **continuous process.** Regular policy and audit reviews, technological and organizational developments within and outside the institute make it necessary to periodically review whether the University of Twente is still on the right course to safeguard security. Audits make it possible to check the policy and the measures taken in terms of their effectiveness and efficiency (**verifiability**).
- **Ownership of information.** As legal entity, the University of Twente owns the information produced under its responsibility unless agreed otherwise for e.g. a study. Furthermore, it manages information of which copyright belongs to third parties. Staff and students must be properly informed about legislation regarding the use or reuse of this information.
- **Valuation of information.** Everyone should be aware of the value of information and act accordingly. This value is determined by any damage resulting from loss of availability, integrity or confidentiality. Classification may be useful in this respect; see the next subsection.

3.3 Classification

Handling information is essential to the proper operation of the University of Twente. Students and staff should be able to trust that information is accessible when and wherever necessary, that it is correct and complete and only available to authorized persons.

Not all information is confidential. Protecting non-confidential information to the same strict degree as highly confidential information is not user-friendly. Proportionality is key, also in the interest of using the available financial resources efficiently. It makes sense to differentiate levels of protections. A useful way to do this is by classifying information.

At the University of Twente, all information to which the Information Security Policy applies is classified on the basis of the quality aspects *Availability*, *Integrity* and *Reliability*.

The level of security measures appropriate for a certain information system depends on the classification of the information processed by the system. A three-grade scale (*Standard, Sensitive, Critical*) is used for the classification for each quality aspect.

The classification must be determined by or on behalf of the owner of the relevant information or of the relevant information system. The Executive Board has appointed custodians (directors of service departments) to fulfil the role of owner for the University of Twente's institutional systems. A description and elaboration of the security levels can be found in the Classification Guideline Information and Information Systems of the University of Twente,[9] which also includes a description of the classification methodology.

[9] Classification Guideline Information and Information Systems of the University of Twente, reference SECR/IM/11/0412/khv, see www.utwente.nl/nl/cyber-safety/cybersafety-map/Wetgeving-map/classificatierichtlijn-ut.pdf (only available in Dutch)

4 Information Security Policy Governance

The good, efficient, and responsible leadership of an organization is often referred to with the term *governance*. This primarily covers the relationship with the most important stakeholders of the institute, such as the students, staff members, and society as a whole. Good governance ensures that all stakeholders know their rights and obligations and act accordingly.

4.1 Harmonization with adjoining policy areas

One aspect of governance is that all sorts of risks and their interconnectedness are awarded appropriate attention. This is referred to as Integral Safety. Physical security, occupational and environmental safety are not taken into consideration here.

The issues concerning privacy — the proper processing of personal information — form part of information security. At the same time, it entails so many specific elements that a separate policy will be drafted on this topic at the end of 2015.

Operation continuity partly falls within the domain of information security but is primarily a line responsibility. Units must draw up plans for operational continuity of the operational processes for which they are responsible.

4.2 Documents

An overview of current policy documents in the area of information security has been included in Appendix B. All established policy documents will be published on the Cybersafety website.[10]

To set the necessary security requirements and procedures requires specific security rules in subareas. The security rules are listed in Appendix C. Through the formal establishment of these security rules, the implementation of the Information Security Policy is made verifiable.

General information about information security is provided by ICTS. Specific work instructions are given to staff in line with their role.

All contracts with suppliers include a subsection on information security.

4.3 Organization of the information security position

Information security is inextricably linked to the provision of information. Except for some specific positions, which will be discussed later, governance coincides with the IT governance as discussed in “Working towards demand-driven IT and information provision.” [11]The terms of the information security positions used here are in alignment, where possible, with those of the Platform for Information Security (PvIB).[12]

The *Information Security Officer* is a role at **strategic** and tactical level within University Information Management. University Information Management advises the Executive Board after coordinating with the ICTS service centre and any custodians of the information systems in question. In terms of information security, the Security Officer monitors the implementation of the Information Security Policy within the institute.

The *Information Security Manager* is an ICTS official and fulfils a role in converting the strategic plans to **tactical** and operational plans. For the service departments this responsibility lies with the system custodian who will usually have delegated the task to the *head of functional management.* For the faculties this responsibility lies with the faculty IT portfolio holder.

[10] www.utwente.nl/en/cyber-safety
[11] Working towards demand-driven IT and information provision, reference SB/UIM/12/0915/evs, seewww.utwente.nl/uim/it-governance/vraagsturing-ict-informatievoorziening.pdf (only available in Dutch)
[12]Positions in information security. Platform for Information Security (PvIB), 2006

At **operational** level, ICTS staff and functional managers are consulted about the implementation of information security measures, among other things. The Information Security Manager is the coordinator of the CERT-UT (Computer Emergency Response Team of the University of Twente).

Securing information systems, including the expenses thereof, forms an integral part of responsible management of the information system in question. Security expenses for workplaces are an integral part of workplace expenses. Information and training for specific applications or target groups are paid for using decentralized funds.

4.3.1 The Executive Board

The Executive Board has final responsibility for information security within the University of Twente and establishes policy and basic measures in the field of information security. Substantive responsibility for information security has been mandated to the Information Security Officer. This officer is tasked with ensuring the security of information across the whole institute.

4.3.2 Information security portfolio holders

The portfolio holder for information security is the member of the Executive Board tasked with IT. He/she has final responsibility for information security within the University of Twente.

4.3.3 Information Security Officer

The Information Security Officer forms part of University Information Management and operates at strategic and tactical level. In conjunction with the head of Information Management, he/she advises the Executive Board. The Information Security Officer draws up Information Security Policy, helps to convert this for the institute's units, monitors compliance (harmonized) and reports on gaps, inconsistencies and deficiencies. An annual security report is drawn up for the Executive Board.

4.3.4 Information Security Manager

The Information Security Manager works within ICTS and fulfils a role in converting strategic plans to tactical and operational plans. He does so in consultation with the Information Security Officer. He coordinates the CERT (Computer Emergency Response Team) of the University of Twente. In addition, he advises on specific information security measures in projects. A management report is drawn up each quarter for the Information Security Officer, the head of Information Management and the ICTS MT.

4.3.5 System Custodian

The System Custodian[13] is responsible for ensuring that the application provides adequate support to the business processes for which the system custodian is responsible. This means that the System Custodian ensures that the application continues to satisfy the requirements and wishes of the users as well as the demands of legislation and regulations and of the Information Security Policy, both now and in the future.

The System Custodian can be supported in this task by the Information Security Officer.

4.3.6 Manager

Compliance with Information Security Policy forms part of the integrated operational management. Every manager has the duty to:

- ensure that his staff members are aware of security policy and the aspects of the security policy that are relevant to them;

[13] See also the memorandum 'Houderschap van een instellingssysteem', reference SB/UIM/15/2801/EVS, www.utwente.nl/uim/it-governance/houderschap-van-een-instellingssysteem.pdf (only available in Dutch)

- ensure compliance with the security policy by staff members;
- periodically bring the issue of information security to the attention of staff members during work discussions;
- be available as point of contact for all staff-related information security matters.

The System Custodian can be supported in this task by the Information Security Manager and the Information Security Officer.

4.3.7 Data Protection Officer

Within the University of Twente, the Data Protection Officer supervises the application of and compliance with the Dutch Personal Data Protection Act (Wbp). The statutory duties and powers of the Data Protection Officer give this official an independent position within the organization.

4.4 Compliance and awareness

Compliance is guaranteed by general supervision of the daily practice of the security management process. It is important in this respect that managers take responsibility and call staff members to account if they fall short.

The Information Security Officer monitors the extent to which the organization has implemented the Information Security Policy. The SURFaudit standards framework[14] is used as a starting point for internal and external audits. An ISO 27001/27002 certification will not be pursued.

Policy and measures are not sufficient to exclude risks in the field of information security. In practice, people often prove to be the most significant risk factor. That is why security risks and measures are periodically brought to everyone's attention, to increase the awareness of risks and encourage safe and responsible conduct. Awareness campaigns regularly organized for staff, students, and third parties are an important part of the implementation of information security policies. These campaigns can converge with national campaigns for higher education, where possible in coordination with safety campaigns for occupational safety, environmental and physical security.

Increasing awareness for security is the responsibility of the managers and the Information Security Officer and the Information Security Manager.

4.4.1 Working group for implementation

To raise awareness and to influence the behaviour of staff and students regarding information security and privacy, a working group will be set up by University Information Management. The working group will draw up an Action Plan and consists of at least the following members:

- Information Security Officer (University Information Management)
- Information Security Manager (ICTS)
- HR Policy Officer (HR)
- Communications Officer (Marketing & Communication department)

[14] The SURFaudit standards framework is based on ISO 27002.

5 Reporting and handling incidents

The management and registration of incidents involves the manner in which information security breaches, detected or suspected by staff and students, are reported and the way in which these are subsequently handled.

It is important to learn from incidents. Incident registration and periodic reports on incidents that have occurred is part of a mature information security environment. For that reason a reporting centre has been set up at the University of Twente and information has been published on how to reach it: CERT-UT, het Computer Emergency Response Team UT.

Each unit bears responsibility to detect and report incidents and information security breaches. The line manager, staff member or student must report incidents and breaches immediately to cert@utwente.nl or via the central ICTS service desk.

There is a responsible disclosure policy, established by the Executive Board. In this policy, the University of Twente offers possible reporters of security gaps in our information systems the guarantee that the University of Twente will, under certain conditions, not take legal steps against them.

Incidents are handled and are discussed in the relevant operational meetings and with the Executive Board if the business process, finances or good reputation are at stake. If disturbing trends are detected, immediate action can be taken in response, for example by taking additional measures or holding an awareness campaign.

The purpose of CERT-UT is to prevent information security incidents where possible and to counter them as soon as they appear and thus to support the continuity of the University of Twente and protect its reputation. CERT-UT also deals with security incidents outside the University of Twente if its own staff or students are in any way involved. In these cases, the SURFcert services, which are globally connected to other CERTs, will be used.

The members of CERT-UT are appointed by the director of ICTS and operate on his instructions. CERT-UT may, in the event of serious incidents, escalate to the portfolio holder of information security through the ICTS director. CERT-UT is led by the Information Security Manager.

CERT-UT is authorized to order a temporary isolation of system/network users, computer systems or network segments in order to be able to carry out its task.

These matters are further detailed in the specific security rules for Security Incident and Event Management.

Appendix A Legislation

At the University of Twente, the relevant legislation and regulations are dealt with in the following manner. This list is not exhaustive.

i. Higher Education and Scientific Research Act (WHW)

The University of Twente has a quality assurance system, assuring amongst other things that data in the student administration records are handled carefully, along with the course results. In addition, the integrity codes for scientific research are also applied and adhered to.

ii. Personal Data Protection Act (Wbp)

Through the information security policy, the University of Twente has implemented the legal privacy requirements (correct and accurate data and adequate technical and organizational measures against loss and wrongful processing). By observing the security measures the university complies with the law.

At the end of 2015, the Privacy policy will be developed in greater detail.

iii. Public Records Act

The University of Twente adheres to the provisions relating to the retention periods as set out in the Public Records Act, for example, and the Public Records Decree regarding the manner in which information recorded in documents (digital or otherwise), information systems, websites, etc. must be handled. It is a periodic part of external accountants' reports.

iv. Copyright Act

The University of Twente does not distribute original works without first having obtained the approval of the owner of the copyright. This means that the University of Twente opposes the use of software without the correct licences.

On its website, the library provides practical information on how to deal with copyright. ICTS manages the software licences.[15]

v. Telecommunications Act

The University of Twente does not have a public section in its network. UT-net is available for a closed group of people involved in education and research and provides access to relevant services. Most legislation from the Telecommunications Act is therefore not applicable. Legislation on net neutrality is applicable where it concerns student accommodation.

vi. Intelligence and Security Services Act

A proposed amendment to the Intelligence and Security Services Act will shortly be discussed in Parliament. If this amendment is adopted, service departments such as the General Intelligence and Security Service and Military Intelligence and Security Service will be granted the right to intercept data traffic from the Internet. The impact on the University of Twente will have to be examined, preferably at SURF level.

[15] www.utwente.nl/nl/cyber-safety/cybersafety-map/Wetgeving-map/softwarelicenties-en-de-ut.pdf (only available in Dutch)

vii. Computer Crime Act

The Computer Crime Act is aimed at the criminal problem areas related to the use of computers. The Act consists of Sections that have been added to the Dutch Criminal Code in various places. The additional sections pertain to:

- Destruction and rendering unusable
- Intercepting data
- *Denial of service*, denial of service attack
- Computer intrusion
- What is computer crime?
- Using a service without payment
- Malware, malicious software

Compliance with this Information Security Policy and implementation of the security rules ensure that the University of Twente has a basic level of security. In the event attacks take place at the University of Twente that penetrate this security to a significant extent and that fall under the Computer Crime Act, the University of Twente will in principle file a report with the police. The Security Manager and Security Officer will advise the Executive Board in this regard as only the Executive Board is entitled to take the decision to file a police report.

Appendix B Policy documents

In addition to the Information Security Policy, a number of policy documents and codes of conduct in the field of information security have been drawn up. All established policy documents will be published on the Cybersafety website.[16]

1. *Classification Guideline Information and Information Systems of University of Twente.*[17]The classification of information provides an estimate of the level of sensitivity and importance of the information and the corresponding degree of security. It concerns protection at the level appropriate to the risks posed for the information in question.
2. *Codes of conduct for IT and internet use at the University of Twente for staff*[18] *and for students.*[19]The codes of conduct indicate the way in which the University of Twente expects IT and internet facilities to be used. The codes regulate the responsible use of IT and internet facilities and the way in which checks take place.
3. *University of Twente Code of conduct for ICT officials*.[20] On the basis of their position, IT officials often have far-reaching powers in the information-processing systems. They are often able to collect privacy-sensitive information quite easily using the tools available to them.
4. *University of Twente Policy Rules on Identity Management*[21]As the custodian, ICTS is responsible for the Identity Management System (IDM). The IDM systems ensures authentication of users of the information systems.
5. *University of Twente Password Policy.*[22]In drafting the Policy Rules for Identity Management at the University of Twente, the decision was taken to draw up a separate password policy in which all aspects would again be considered carefully and developed further. The different viewpoints are detailed in this document.
6. *University of Twente Authorization Policy*[23]Granting rights to who may do what is referred to as authorization. The Authorization Policy sets general guidelines on how to deal with authorizations in information systems.
7. *Ambition Level SURFaudit.*[24]At SURF level, the institutes agreed to conduct the SURFaudit to measure the level of information security. The Executive Board decided to establish the level for the SURFaudit at a minimum maturity level 3: Defined Process.

[16] www.utwente.nl/en/cyber-safety
[17] See www.utwente.nl/nl/cyber-safety/cybersafety-map/Wetgeving-map/classificatierichtlijn-ut.pdf (only available in Dutch)
[18] See www.utwente.nl/en/cyber-safety/cybersafety-map/legislation-map/gedragscode-ict-mw-en.pdf
[19] See www.utwente.nl/en/cyber-safety/cybersafety-map/legislation-map/gedragscode-ict-stud-en.pdf
[20] See www.utwente.nl/nl/cyber-safety/cybersafety-map/Wetgeving-map/gedragscode-ict-functionarissen.pdf (only available in Dutch)
[21] See www.utwente.nl/nl/sb/beleidsterreinen/universitair-informatiemanagement/informatiebeveiliging/beleidsregels-identitymanagement-universiteit-twente.pdf (only available in Dutch)
[22] See www.utwente.nl/en/cyber-safety/cybersafety-map/legislation-map/wachtwoordbeleid-universiteit-twente-engels-def.pdf
[23] See www.utwente.nl/uim/informatiebeveiliging/autorisatiebeleid-universiteit-twente.pdf (only available in Dutch)
[24] See www.utwente.nl/uim/informatiebeveiliging/ambitieniveau-surfaudit.pdf (only available in Dutch)

Appendix C Security rules

To determine the necessary security requirements and procedures, specific security rules are required for subareas. Through the formal establishment of these security rules, their implementation is made verifiable. ICTS staff can generally limit themselves to the security rules that are relevant to them.

The Security Rules replace the Security Policies established in 2008.

In the following subareas, specific security rules have been established:

1. *Means of authentication*, management and use of passwords, software and/or hardware keys. See page 16.
2. *Basic IT facilities* such as email, data storage, telephony and chat. See page 17.
3. *Data centres* including the servers installed in them. See page 18.
4. *Hardware*, the entire life cycle from purchase to phase-out. See page 19.
5. *Information systems*, the entire life cycle from acquisition to phase-out. See page 20.
6. *Network*, including the active network components such as routers, switches, hubs, access points, etc. See page 21.
7. *Security Incident and Event Management*, CERT-UT working practice and handling of security incidents. See page 22.
8. *Workplaces* for users. See page 23.

Security rules – means of authentication

Introduction

The Information Security Policy indicates that specific security rules are necessary in subareas. One of these subareas relates to management and use of means of authentication. In order to gain access to certain IT facilities, authentication requires, besides a username, the use of a password, software and/or hardware key.

Related relevant statements are made in the Code of Conduct for IT and Internet Use, Identity Management Policy rules, Password Policy and Authorization Policy[25], which will not be repeated here.

Responsibility

1. ICTS bears responsibility for the means of authentication.
2. For all types of authentication, an auditable procedure is in place relating to providing, use, replacement, withdrawal and loss.

Purpose limitation

3. Means of authentication are personal, device-specific or application-specific.
4. Personal means of authentication are private and cannot be transferred.
5. One person is always responsible for all device-specific and application-specific means of authentication. He or she manages the relevant means and monitors its use. ICTS registers who is responsible for which means of authentication.

Passwords

6. Personal passwords require a certain level of complexity. ICTS will publish a guideline that further details this requirement and will ensure its application.
7. Device-specific and application-specific passwords are highly complex and have a high entropy. ICTS will publish a guideline that further details this requirement and will ensure its application.
8. Default passwords as set by the supplier must be changed.

[25]See the University Information Management website and the Cybersafety website for the documents mentioned www.utwente.nl/en/sp/policy/information_management/ / www.utwente.nl/en/cyber-safety

Security rules – Basic IT-facilities

Introduction

The Information Security Policy indicates that specific security rules are necessary in subareas. One of these subareas relates to basic IT facilities such as email, data storage, telephony and chats. These rules are set down in this document.

Responsibility

1. ICTS is custodian for the basic IT facilities provided centrally and is responsible for compliance with the security rules.
2. On the website, ICTS offers information on the safe use of the IT facilities.

Provisioning

3. When an account is provided, the user is immediately informed about security, including by being notified of the Code of Conduct for IT and Internet Use.[26]

Data

4. Access to a user's data, including messages, configuration and metadata, is only permitted on the approval of the user in question or on the written instructions of the Executive Board, as set down in the Code of conduct. This access will be registered in all cases.
5. All data transport must comply with the encryption measures as set out in the Classification Guideline.[27]

Email

6. All senders (whether person or application) of emails sent by the University of Twente must be traceable.
7. Incoming or outgoing emails are checked for malware and spam and where necessary the email is partly or entirely deleted or set apart.
8. The number of addressees and the size of the emails are limited to a reasonable maximum. The details are published by ICTS on the website.

[26]Code of Conduct for IT and Internet Use,
see www.utwente.nl/en/cyber-safety/cybersafety-map/legislation-map/gedragscode-ict-mw-en.pdf
[27]Classification Guideline Information and Information Systems,
see www.utwente.nl/nl/cyber-safety/cybersafety-map/Wetgeving-map/classificatierichtlijn-ut.pdf (only available in Dutch)

Security rules – Data centres

Introduction

The Information Security Policy indicates that specific security rules are necessary in subareas. One of these subareas relates to the data centres including the servers installed in them. These rules are set down in this document.

Responsibility

1. ICTS is responsible for the data centres, including emergency power, cooling, etc.
2. ICTS enters into conclusive agreements with suppliers such as FSC and SURFnet.
3. ICTS is responsible for its own servers in the data centres and enters into conclusive agreements with the owners of the other servers.

Access

4. Access to the data centres is only permitted to install, repair, replace or remove hardware and to carry out maintenance to the data facility itself.
5. ICTS will set further guidelines for access to the data centres in accordance with the Authorization Policy[28].
6. All access to the data centres is logged.

Servers

7. ICTS logs all servers installed and registers the purpose, administrator and substitute of each server. A clearly legible registration number is attached to the server.
8. Processes and ports not necessary for the server's use are disabled.
9. Any server which disrupts the UTnet or other IT service, or otherwise causes a security incident, will be disabled or isolated by order of CERT-UT.

Management

10. The technical management of applications and servers is conducted on a network that is obviously separate from the user network.
11. Separate personal management accounts are used for this management.
12. The use of management accounts is logged.
13. The management of management accounts adheres to the Authorization Policy.

[28] www.utwente.nl/uim/informatiebeveiliging/autorisatiebeleid-universiteit-twente.pdf (only available in Dutch)

Security Rules - Hardware

Introduction

The Information Security Policy indicates that specific security rules are necessary in subareas. One of these subareas relates to hardware life cycle, from purchase to phase out. These rules are set down in this document.

Responsibility

1. The custodian or owner of a system also bears responsibility for the hardware and compliance with the security rules.
2. If ICTS conducts the technical management, ICTS is also responsible for compliance with these rules.
3. If an information system operates on ICTS infrastructure, ICTS will bear responsibility for that hardware, not the custodian or owner of the information system.

Purchase

4. All hardware that can be connected to the UT network requires a certain degree of security. The Security Manager manages these minimum requirements and publishes them on the ICTS website.
5. In the event that a lot of hardware or important hardware is to be purchased, the Security Manager will be involved in the purchase process in a timely fashion.

Management

6. Default passwords as set by the supplier must be changed.
7. In the event of incidents, the party responsible must be accountable. To this end, ICTS logs all hardware connected to the UT network, or logs the account with which the UT network is accessed.
8. If a firmware update would resolve a security issue, it must be carried out within a reasonable period.

Phase-out

9. When data carriers such as hard discs, tapes, mobile devices, USB sticks etc. are put out of operation or disposed of, the data on them must be adequately destroyed by or on behalf of the owner. Through the website, ICTS offers information about the way in which this can be done for each type of data carrier.

Security Rules - Information Systems

Introduction

The Information Security Policy indicates that specific security rules are necessary in subareas. One of these subareas relates to the information systems' life cycle, from acquisition to phase out. These rules are set down in this document. Not bound to these rules is software that has been purchased for individual users, where Availability, Integrity and Confidentiality is not relevant.

Responsibility

1. The custodian[29] or owner of an information system is responsible for compliance with the security rules.
2. When ICTS conducts the technical and/or application management, agreements regarding security and compliance with these rules will be laid down in the Service Level Agreement with the custodian.
3. Access to an information system is regulated in accordance with the Authorization Policy.[30]

Acquisition

4. Before or at the start of the project, a classification takes place in line with the Classification Guideline Information and Information Systems[31] so that the results can help determine the requirements for the information system.
5. When using cloud services, the SURF Legal standards framework for cloud services in higher education[32] is applied.
6. Each project plan for the purchase or development of software will include a section on security. The Security Manager manages a generic overview of key issues for these sections and publishes them on the ICTS website.

Management

7. Security issues are resolved in software developed by the University of Twente.
8. Patches and updates from suppliers are carried out systematically.
9. Where appropriate, roles are separated; for instance, developers have no rights to the production environment.

Logging

10. Logging is kept to a minimum.
11. The custodian logs the objectives and retention periods of the log files of all information systems under his responsibility.

[29] See also www.utwente.nl/uim/it-governance/houderschap-van-een-instellingssysteem.pdf (only available in Dutch)
[30] See www.utwente.nl/uim//informatiebeveiliging/autorisatiebeleid-universiteit-twente.pdf (only available in Dutch)
[31] See www.utwente.nl/nl/cyber-safety/cybersafety-map/Wetgeving-map/classificatierichtlijn-ut.pdf (only available in Dutch)
[32] See www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2016/legal-standards-framework-for-cloud-services

Phase-out

12. Software no longer supported is phased out, unless this is not possible and only if appropriate measures sufficiently limit the security risks.
13. The conversion, archiving and destruction of data is also considered during phase-out.

Security rules – Network

Introduction

The Information Security Policy indicates that specific security rules are necessary in subareas. One of these subareas relates to the network, including the active network components such as routers, switches, hubs, access points, etc. These rules are set out in this document.

Responsibility

1. ICTS is responsible for the network, including all active network components such as routers, switches, hubs, access points, etc.
2. Where possible, active network components are placed in an enclosed room.
3. ICTS logs all active network components.
4. The University of Twente starts from the basic premise of an open network, in principle without restrictions to internet traffic.
5. The University of Twente complies with the agreements made with SURFnet.

Own equipment

6. In principle, ICTS only ensures the installation of network equipment. ICTS logs the exceptions including the written agreements made.
7. ICTS logs third party connections, including the agreements made.
8. Any equipment which disrupts the UT-net or other IT service, or otherwise causes a security incident will be disabled or isolated by order of CERT-UT. This also applies to equipment that disrupts the use of the wireless network.

Campus

9. Campus residents may install their own routers, etc.
10. If a campus resident's router disrupts one of the systems behind the UTnet router, disrupts another IT service, or otherwise causes a security incident, it will be disabled or isolated by order of CERT-UT.

Management

11. The network components are managed through a separate management network or as a minimum, through a secure connection.
12. Access to network components is regulated in accordance with Authorization Policy.[33]

[33] See www.utwente.nl/uim/informatiebeveiliging/autorisatiebeleid-universiteit-twente.pdf (only available in Dutch)

Security rules - SIEM (Security Incident and Event Management)

Introduction

The Information Security Policy indicates that specific security rules are necessary in subareas. One of these subareas relates to the working practice of CERT-UT and the handling of security incidents. These rules are set down in this document.

Responsibility

1. ICTS is responsible for the installation and operation of CERT-UT as laid down in the Information Security Policy.
2. The Security Manager bears responsibility for Security Incident and Event Management.

Incidents

3. Incidents are immediately reported to CERT-UT directly or through the ICTS helpdesk.
4. CERT-UT uses standard procedures to log and remedy incidents.
5. A specific procedure applies to security emergencies.
6. Reports are dealt with confidentially.

Events

7. Any actions, acts or events that could influence the security of information are identified and recorded. If an event influences operational management it will be reported as an incident.

Preventive measures

8. The Security Managers provides information to users, developers and administrators to prevent security incidents.
9. The Security Manager may provide solicited and unsolicited advice on possible security issues.

Reports

10. Each quarter, the Security Manager provides the Security Officer with a management report about the incidents and events identified and the advice issued.
11. This report contains in any case all security emergencies and identified trends.

Security rules – Workplaces

Introduction

The Information Security Policy indicates that specific security rules are necessary in subareas. One of these subareas relates to users' workplaces. These rules are set down in this document.

Responsibility

1. ICTS is responsible for the security of the workplaces in so far as these are managed by ICTS.
2. Users are responsible for the security of their own workplace in so far as this is not managed by ICTS. Security information and resources can be found through the ICTS website.

Management

3. Separate personal management accounts are used for management by ICTS.
4. The use of management accounts is logged.
5. The management of management accounts adheres to the Authorization Policy.[34]

Users

6. Staff will never ask users to provide their password. If necessary, users will be asked to log on.
7. Users are periodically informed by ICTS about security, and they are notified of the Code of Conduct for IT and Internet Use.[35]

Malfunctions

8. Any workplace which disrupts the UTnet or other IT service, or otherwise causes a security issue will be disabled or isolated by order of CERT-UT.

[34] See www.utwente.nl/uim/informatiebeveiliging/autorisatiebeleid-universiteit-twente.pdf (only available in Dutch)
[35]Code of Conduct for IT and Internet Use,
See www.utwente.nl/en/cyber-safety/cybersafety-map/legislation-map/gedragscode-ict-mw-en.pdf