# Information Security Policy

## Best Practice Document

Produced by UNINETT led working group on security
(No UFS126)

Authors: Kenneth Høstland, Per Arne Enstad, Øyvind Eilertsen, Gunnar Bøe
October 2010

Document No: GN3-NA3-T4-UFS126
Version / date: October 2010
Original language: Norwegian
Original title: “UFS126: Informasjonsikkerhetspolicy”
Original version / date: July 2010
Contact: campus@uninett.no

UNINETT bears responsibility for the content of this document. The work has been carried out by a UNINETT led working group on security as part of a joint-venture project within the HE sector in Norway.



The translation of this report has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 238875, relating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3)'.



# Table of Contents


EXECUTIVE SUMMARY 4

INTRODUCTION 5

1 INFORMATION SECURITY POLICY 6

1.1 Security goals 6

1.2 Security strategy 6

2 ROLES AND AREAS OF RESPONSIBILITY 8

3 PRINCIPLES FOR INFORMATION SECURITY AT <X UNIVERSITY> 10

3.1 Risk management 10

3.2 Information security policy 11

3.3 Security organization 11

3.4 Classification and control of assets 12

3.5 Information security in connection with users of <X University>'s services 13

3.6 Information security regarding physical conditions 14

3.7 IT communications and operations management 17

3.8 Access control 21

3.9 Information systems acquisition, development and maintenance 22

3.10 Information security incident management 23

3.11 Continuity planning 24

3.12 Compliance 25

4 GOVERNING DOCUMENTS FOR SAFETY WORK 27

4.1 Purpose of governing documents 27

4.2 Document structure 27

REFERENCES 28

# Executive Summary

Information management is an essential part of good IT governance, which in turn is a cornerstone in corporate governance. An integral part of the IT governance is information security, in particular pertaining to personal information. However, many organisations do not have a clear policy for information security management.

This document contains a template of an information security policy. The template is developed by UNINETT as part of the GigaCampus project and has been used in processes to aid universities and university colleges in Norway with getting an information security in place. The security policy template combines legal requirements and current best practice for an information security management policy for Norwegian universities and university colleges. It provides a policy with information security objectives and strategy, and defines roles and responsibilities.

Core principles for information security management, as defined in ISO/IEC 27002, are adapted to the local situation for the following areas:

- Risk assessment
- Organising information security
- Asset management
- Human resources security
- Physical security
- Communications and operations management
- Access control
- System development and maintenance
- Information security incident management
- Business continuity management
- Compliance

Governing documents for Information Security Management are also defined.

The foundation for this best practice is ISO/IEC 27001 and ISO/IEC 27002 which have been condensed to a manageable and applicable level (25-30 pages as opposed to the 108 pages of ISO/IEC 27002). Norwegian legal requirements have also been fulfilled. The EU equivalents can be found in:

- Directive 95/46/EC (Data Protection Directive)
- Directive 2002/58/EC (the E-Privacy Directive)
- Directive 2006/24/EC Article 5 (The Data Retention Directive)

# Introduction

The rest of this document (chapters 1-4) contains a UNINETT developed template for an information security policy. It is based on ISO/IEC 27001 and ISO/IEC 27002 and has been condensed to a manageable and applicable level (25-30 pages as opposed to the 108 pages of ISO/IEC 27002). UNINETT has been using this template in ongoing processes with universities and university colleges in Norway. The work started in 2008 as part of the GigaCampus project. The situation at the time was that most of the institutions did not have a formally approved and implemented security policy in place. So far UNINETT has visited a total of 27 institutions and of these approx. 15 institutions now have an approved security policy.

UNINETT's role in the process has been as catalyst motivating the local project teams to develop their own policy. The importance of involvement from top management has been stressed from day one. The security policy should be signed by the manager (chancellor/president) of the institution, or whoever has the legal responsibility according to local legislation.

The policy template has been used as a starting point in the process of developing a locally agreed security policy. Local involvement and ownership to the policy is a key to its success. In many ways the process itself is more important than the final document.

In addition to the information security policy the institution need to develop a number of underlying documents detailing how the various aspects of the policy should be implemented. These are not dealt with in the present document.

# 1 Information security policy

## 1.1 Security goals

<X University> is committed to safeguard the confidentiality, integrity and availability of all physical and electronic information assets of the institution to ensure that regulatory, operational and contractual requirements are fulfilled. The overall goals for information security at <X University> are the following:

- Ensure compliance with current laws, regulations and guidelines.
- Comply with requirements for confidentiality, integrity and availability for <X University>'s employees, students and other users.
- Establish controls for protecting <X University>'s information and information systems against theft, abuse and other forms of harm and loss.
- Motivate administrators and employees to maintain the responsibility for, ownership of and knowledge about information security, in order to minimize the risk of security incidents.
- Ensure that <X University> is capable of continuing their services even if major security incidents occur.
- Ensure the protection of personal data (privacy).
- Ensure the availability and reliability of the network infrastructure and the services supplied and operated by <X University>.
- Comply with methods from international standards for information security, e.g. ISO/IEC 27001.
- Ensure that external service providers comply with <X University>'s information security needs and requirements.
- Ensure flexibility and an acceptable level of security for accessing information systems from off-campus.
- [Other security goals]

## 1.2 Security strategy

<X University>'s current business strategy and framework for risk management are the guidelines for identifying, assessing, evaluating and controlling information related risks through establishing and maintaining the information security policy (this document).

It has been decided that information security is to be ensured by the policy for information security and a set of underlying and supplemental documents (see chapter 0). In order to secure operations at <X University> even after serious incidents, <X University> shall ensure the availability of continuity plans, backup procedures, defence against damaging code and malicious activities, system and information access control, incident management and reporting.

The term information security is related to the following basic concepts:

- ***Confidentiality:***
  The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- ***Integrity:***
  The property of safeguarding the accuracy and completeness of assets.
- ***Availability:***
  The property of being accessible and usable upon demand by an authorized entity.

Some of the most critical aspects supporting <X University>'s activities are availability and reliability for network, infrastructure and services. <X University> practices openness and principles of public disclosure, but will in certain situations prioritize confidentiality over availability and integrity.

Every user of <X University>'s information systems shall comply with this information security policy. Violation of this policy and of relevant security requirements will therefore constitute a breach of trust between the user and <X University>, and may have consequences for employment or contractual relationships.

……
Chancellor/President of <X University>

# 2 Roles and areas of responsibility

The administration has the overall responsibility for managing <X University>'s values in an effective and satisfactory manner according to current laws, requirements and contracts.

The Chancellor/President has the overall responsibility for information security at <X University>, including information security regarding personnel and IT security.

### 2.1.1 Owner of the security policy

The Chancellor/President is the owner of the security policy (this document). The Chancellor/President delegates the responsibility for security-related documentation to the CSO (Chief Security Officer). All policy changes must be approved and signed by the CSO.

### 2.1.2 Chief Security Officer (CSO)

The Chief Security Officer (CSO) holds the primary responsibility for ensuring the information security at <X University>. [...] has this role (see chapter 0).

### 2.1.3 System owner

The system owner, in consultation with the IT department, is responsible for purchasing requirements, development and maintenance of information and related information systems. All systems and all types of information must have a defined owner. The system owner must define which users or user groups are allowed access to the information and what authorized use of this information consists of. The system ownership shall be described in a separate document [REF].

### 2.1.4 System administrator

System administrators are persons administrating <X University>'s information systems and the information entrusted to the university by other parties. Each type of information and system may have one or more dedicated system administrators. These are responsible for protecting the information, including implementing systems for access control to safeguard confidentiality, and carry out backup procedures to ensure that critical

information is not lost. They will further implement, run and maintain the security systems in accordance with the security policy. Each system must have one or more system administrators. This shall be documented.

### 2.1.5 Users

Employees and students are responsible for getting acquainted and complying with <X University>'s IT regulations. Questions regarding the administration of various types of information should be posed to the system owner of the relevant information, or to the system administrator.

### 2.1.6 Consultants and contractual partners

Contractual partners and contracted consultants must sign a confidentiality agreement prior to accessing sensitive information. The System owner is responsible for ensuring that this is implemented.

# 3 Principles for information security at <X University>

## 3.1 Risk management

### 3.1.1 Risk assessment and management

**3.1.1.1** *<X University>'s approach to security should be based on risk assessments.*

**3.1.1.2** *<X University> should continuously assess the risk and evaluate the need for protective measures. Measures must be evaluated based on <X University>'s role as an establishment for education and research and with regards to efficiency, cost and practical feasibility.*

**3.1.1.3** *An overall risk assessment of the information systems should be performed annually.*

**3.1.1.4** *Risk assessments must identify, quantify and prioritize the risks according to relevant criteria for acceptable risks.*

**3.1.1.5** *Risk assessments are to be carried out when implementing changes impacting information security. Recognized methods of assessing risks should be employed, such as ISO/IEC 27005.*

**3.1.1.6** *The CSO is responsible for ensuring that the risk management processes at <X University> are coordinated in accordance with the policy.*

**3.1.1.7** *The system owners are responsible for ensuring that risk assessments within their area of responsibility are implemented in accordance with the policy.*

**3.1.1.8** *Risk management is to be carried out according to criteria approved by the management at <X University>.*

**3.1.1.9** *Risk assessments must be approved by the management at <X University> and/or the system owners.*

**3.1.1.10** *If a risk assessment reveals unacceptable risks, measures must be implemented to reduce the risk to an acceptable level.*

## 3.2 Information security policy

**3.2.1.1** *The Chancellor/President shall ensure that the information security policy, as well as guidelines and standards, are utilized and acted upon.*

**3.2.1.2** *The Chancellor/President must ensure the availability of sufficient training and information material for all users, in order to enable the users to protect <X University>'s data and information systems.*

**3.2.1.3** *The security policy shall be reviewed and updated annually or when necessary, in accordance with principles described in ISO/IEC 27001.*

**3.2.1.4** *All important changes to <X University>'s activities, and other external changes related to the threat level, should result in a revision of the policy and the guidelines relevant to the information security.*

## 3.3 Security organization

### 3.3.1 Security organization in <X University>

[This chapter *must* be adapted to local requirements]

Security responsibility is distributed as follows:

- The Chancellor/President is primarily responsible for the security and is the controller according to the 95/46/EC, Article 2 (d).
- The Chancellor/President is responsible for all government contact.
- The security authority at <X University>, including information security and IT security, has been delegated to […]. […] is hereby appointed CSO (Chief Security Officer) at <X University>.
- Each department and section is responsible for implementing the unit's information security. The managers of each unit must appoint separate security administrators.
- The Chancellor for education has the primary responsibility for the information security in connection with the student registry and other student related information.
- The IT Director has executive responsibility for information security in connection with IT systems and infrastructure.
- The Operations manager has executive responsibility for information security in connection with structural infrastructure.
- The Personnel director has executive responsibility for information security according to the Personal Data Act and is the controller on a daily basis of the personal information of the employees.

- The Personnel director has executive responsibility for information security related to HSE systems.
- The Chancellor for Academic Affairs and Research Administration has executive responsibility for research related personal information.
- The Operations manager has overall responsibility for quality work, while the operational responsibility is delegated according to the management structure.
- Projects should be organized according to <X University>'s project manual, where information security should be defined.
- <X University>'s information security will be revised on a regular basis, through internal control and at need, with assistance from an external IT auditor.

<X University> has established a forum for information security [consisting of e.g. the Chancellor/President, system owners, the HSE manager, the IT security manager and others]. The security forum will advise the Chancellor/President about measures furthering the information security of the organization. The security forum has the following responsibilities, among others:

- Review and recommend information security policy and accompanying documentation and general distribution of responsibility.
- Monitor substantial changes of threats against the information assets of the organization.
- Review and monitor reported security incidents.
- Authorize initiatives to strengthen information security.

## 3.4 Classification and control of assets

#### 3.4.1.1 *"Assets" include both information assets and physical assets.*

#### 3.4.1.2 *Information and infrastructure should be classified according to security level and access control.*

#### 3.4.1.3 *Information as mentioned in item 3.4.1.1 should be classified as one of three categories for confidentiality:*

**Sensitive**

**Information of a sensitive variety where unauthorized access (including internally) may lead to considerable damage for individuals, the university college or their interests. [*Sensitive information is here synonymous with being kept from public access according to the Norwegian Public Administration Act or sensitive personal information as defined by the Personal Data Act. Corresponding national legal requirements may apply.*] This type of information must be secured in "red" zones, see chapter 3.6.**

**Internal**

**Information which may harm <X University> or be inappropriate for a third party to gain knowledge of. The System owner decides who may access and how to implement that access.**

**Open**

**Other information is open.**

**3.4.1.4** *<X University> shall carry out risk analyses in order to classify information based on how critical it is for operations (criticality).*

**3.4.1.5** *Routines for classification of information and risk analysis must be developed.*

**3.4.1.6** *Users administrating information on behalf of <X University> should treat said information according to classification.*

**3.4.1.7** *Sensitive documents should be clearly marked.*

**3.4.1.8** *Classification of equipment according to criticality will be discussed in chapter 3.11.*

**3.4.1.9** *A plan for electronic storage of essential documentation should be developed.*

**3.4.1.10** *Information that is vital for operations should be accessible independent of which systems the information was created or processed in.*

## 3.5 Information security in connection with users of <X University>'s services

### 3.5.1 Prior to employment

**3.5.1.1** *Security responsibility and roles for employees and contractors should be described.*

**3.5.1.2** *A background check is to be carried out of all appointees to positions at <X> according to relevant laws and regulations.*

**3.5.1.3** *A confidentiality agreement should be signed by employees, contractors or others who may gain access to sensitive and/or internal information.*

**3.5.1.4** *IT regulations should be accepted for all employment contracts and for system access for third parties.*

### 3.5.2 During employment

**3.5.2.1** *The IT regulations refer to <X University>'s information security requirements and the users' responsibility for complying with these regulations.*

**3.5.2.2** *The IT regulations should be reviewed regularly with all users and with all new hires.*

**3.5.2.3** *All employees and third party users should receive adequate training and updating regarding the Information security policy and procedures. The training requirements may vary.*

**3.5.2.4** *Breaches of the Information security policy and accompanying guidelines will normally result in sanctions. [Refer to the relevant laws and valid regulations at <X University>.]*

**3.5.2.5** *<X University>'s information, information systems and other assets should only be utilized for their intended purpose. Necessary private usage is permitted.*

**3.5.2.6** *Private IT equipment in <X University>'s infrastructure may only be connected where explicitly permitted. All other use must be approved in advance by the IT department.*

**3.5.2.7** *Use of <X University>'s IT infrastructure for personal commercial activities is [under no circumstances] permitted.*

### 3.5.3 Termination or change of employment

**3.5.3.1** *The responsibility for termination or change of employment should be clearly defined in a separate routine with relevant circulation forms.*

**3.5.3.2** *<X University>'s assets should be handed in at the conclusion of the need for the use of these assets.*

**3.5.3.3** *<X University> should change or terminate access rights at termination or change of employment. A routine should be present for handling alumni relationships.*

**3.5.3.4** *Notification on employment termination or change should be carried out through the procedures defined in the personnel system.*

## 3.6 Information security regarding physical conditions

### 3.6.1 Security areas

**3.6.1.1** *IT equipment and information that require protection should be placed in secure physical areas. Secure areas should have suitable access control to ensure that only authorized personnel have access. The following zones should be utilized:*

| Security level | Area | Security |
|---|---|---|
| **Green** | No access restrictions<br>Student areas and cafeteria. | No access control during ordinary office hours.<br>Internal and sensitive information should not be printed out in this zone. |
| **Yellow** | Areas where internal information may be found during office hours.<br>Offices, meeting rooms, some archives, some technical rooms like labs, printer rooms. | All printouts should be protected with "Follow me" function.<br>Access control: Key card |
| **Red** | Restricted areas requiring special authorization.<br>Computer rooms, server rooms, archives, etc. containing sensitive information. | All printouts should be protected with "Follow me" function.<br>Access control: Key card |

**3.6.1.2** *Zones should be marked on construction drawings or explicitly described in a separate document.*

**3.6.1.3** *The IT security manager is responsible for approving physical access to technical computer rooms.*

**3.6.1.4** *The Physical security manager is responsible for the approval of physical access to areas other than technical computer rooms.*

**3.6.1.5** *All of <X University>'s buildings should be secured according their classification by using adequate security systems, including suitable tracking/logging. See table above.*

**3.6.1.6** *Security managers for the various areas of responsibility should ensure that work performed by third parties in secure zones is suitably monitored and documented.*

**3.6.1.7** *All personnel should be able to be identified and wear personal access cards when present in yellow or red zones. The ID cards are personal, and must not be transferred to a third party or to colleagues.*

**3.6.1.8** *Red zones should be properly secured against damage caused by fire, water, explosions, vibrations, etc.*

**3.6.1.9** *All external doors and windows must be closed and locked at the end of the work day.*

**3.6.1.10** *Access cards may be supplied to workmen, technicians and others after proper identification [and a signed confidentiality agreement].*

**3.6.1.11** *Anyone receiving visitors in the yellow zone is responsible for the supervision of their visitors.*

**3.6.1.12** *Visitors in the red zone must be signed in and out, and must carry visible guest cards or personal access cards.*

**3.6.1.13** *Visitors in the red zone must be escorted [or monitored, e.g. with cameras].*

### 3.6.2 Securing equipment

**3.6.2.1** *IT equipment classified as "high" (see chapter 3.11.1.5) must be protected against environmental threats (fires, flooding, temperature variations, etc.). Classification of equipment should be based on risk assessments.*

**3.6.2.2** *Information classified as "sensitive" must not be stored on portable computer equipment (e.g. laptops, cell phones, memory sticks, etc.). If it is necessary to store this information on portable equipment, the information must be password protected and encrypted in compliance with guidelines from the IT department.*

**3.6.2.3** *During travel, portable computer equipment should be treated as carry-on luggage.*

**3.6.2.4** *Areas classified as "red" must be secured with suitable fire extinguishing equipment with appropriate alarms.*

**3.6.2.5** *Fire drills shall be carried out on a regular basis.*

## 3.7 IT communications and operations management

### 3.7.1 Operational procedures and areas of responsibility

**3.7.1.1** *Purchase and installation of IT equipment must be approved by the IT department.*

**3.7.1.2** *Purchase and installation of software for IT equipment must be approved by the IT department.*

**3.7.1.3** *The IT department should ensure documentation of the IT systems according to <X University>'s standards.*

**3.7.1.4** *Changes in IT systems should only be implemented if well-founded from a business and security standpoint.*

**3.7.1.5** *The IT department should have emergency procedures in order to minimize the effect of unsuccessful changes to the IT systems.*

**3.7.1.6** *Operational procedures should be documented. Documentation must be updated following all substantial changes.*

**3.7.1.7** *Before a new IT system is put in production, plans and risk assessments should be in place to avoid errors. Additionally, routines for monitoring and managing unforeseen problems should be in place.*

**3.7.1.8** *Duties and responsibilities should be separated in a manner reducing the possibility of unauthorized or unforeseen abuse of <X University>'s assets.*

**3.7.1.9** *Development, testing and maintenance should be separated from operations in order to reduce the risk of unauthorized access or changes, and in order to reduce the risk of error conditions.*

### 3.7.2 Third party services

**3.7.2.1** *All contracts regarding outsourced IT systems should include*

- information security requirements, including confidentiality, integrity and availability,
- a description of the agreed security level,
- requirements for reporting security incidents from third parties,
- a description of how <X University> may ensure that third parties are fulfilling their contracts,
- a description of <X University>'s right to audit third parties.

### 3.7.3 System planning and acceptance

**3.7.3.1** *Requirements for information security must be taken into consideration when designing, testing, implementing and upgrading IT systems, as well as during system changes. Routines must be developed for change management and system development/maintenance.*

**3.7.3.2** *IT systems must be dimensioned according to capacity requirements. The load should be monitored in order to apply upgrades and adjustments in a timely manner. This is especially important for business-critical systems.*

### 3.7.4 Protection against malicious code

**3.7.4.1** *Computer equipment must be safeguarded against virus and other malicious code. This is the responsibility of the IT security manager.*

### 3.7.5 Backup

**3.7.5.1** *The IT department is responsible for carrying out regular backups and restore of these backups, as well as data storage on <X University>'s IT systems according to their classification.*

**3.7.5.2** *Backups should be stored externally or in a separate, suitably protected zone.*

### 3.7.6 Network administration

**3.7.6.1** *The IT department has the overall responsibility for protecting <X University>'s internal network.*

**3.7.6.2** *There should be an inventory containing all equipment connected to <X university>'s wired networks.*

**3.7.6.3** *All access to <X University>'s networks should be logged.*

### 3.7.7 Management of storage media

**3.7.7.1** *There should be procedures in place for the management of removable storage media. Implementation is the responsibility of each employee.*

**3.7.7.2** *Storage media should be disposed of securely and safely when no longer required, using formal procedures.*

### 3.7.8 Exchange of information

**3.7.8.1** *Procedures and controls should be established for protecting exchange of information with third parties and information transfer. Third party suppliers must comply with these procedures.*

**3.7.8.2** *<X University> has the right to access personal e-mail and other personal data stored on <X University>'s computer networks [according to the relevant national legal requirements. Norway: Personal Data Act, chapter 9.]*

### 3.7.9 Use of encryption

**3.7.9.1** *Storage and transfer of sensitive information (see class model in chapter 3.11) should be encrypted or otherwise protected.*

### 3.7.10 Electronic exchange of information

**3.7.10.1** *Information exchanged across public networks in connection with e-commerce, should be protected against fraud, contractual discrepancies, unauthorized access and changes.*

**3.7.10.2** *The IT department should ensure that publicly accessible information, e.g. on <X University>'s web services, is adequately protected against unauthorized access.*

### 3.7.11 Monitoring of system access and usage

**3.7.11.1** *Access and use of IT systems should be logged and monitored in order to detect unauthorized information processing activities.*

**3.7.11.2** *Usage and decisions should be traceable to a specific entity, e.g. a person or a specific system.*

**3.7.11.3** *The IT department should register substantial disruptions and irregularities of system operations, along with potential causes of the errors.*

**3.7.11.4** *Capacity, uptime and quality of the IT systems and networks should be sufficiently monitored in order to ensure reliable operation and availability.*

**3.7.11.5** *The IT department should log security incidents for all essential systems.*

**3.7.11.6** *The IT department should ensure that system clocks are synchronized to the correct time.*

**3.7.11.7** *[Usage of information systems containing personal information may be regulated. Check your local legislation…]*

## 3.8 Access control

### 3.8.1 Business requirements

**3.8.1.1** *Written guidelines for access control and passwords based on business and security requirements should be in place. Guidelines should be re-evaluated on a regular basis.*

**3.8.1.2** *Guidelines should contain password requirements (frequency of change, minimum length, character types which may/must be utilized, etc.) and regulate password storage.*

### 3.8.2 User administration and responsibility

**3.8.2.1** *Users accessing systems must be authenticated according to guidelines.*

**3.8.2.2** *Users should have unique combinations of usernames and passwords.*

**3.8.2.3** *Users are responsible for any usage of their usernames and passwords. Users should keep their passwords confidential and not disclose them unless explicitly authorized by the CSO.*

### 3.8.3 Access control/Authorization

**3.8.3.1** *Access to information systems should be authorized by immediate superiors in accordance with the system owner directives. This includes access rights, including accompanying privileges. Authorizations should only be granted on a "need to know" basis, and regulated according to role.*

**3.8.3.2** *The immediate superior should alert the system administrator about granting access and changes in accordance with the directives from the system owner.*

**3.8.3.3** *Roles and responsibilities with accompanying access rights should be described based on the following classifications.*

- Internal (several roles)
- External (several roles)
- Student
- Public
- Others

### 3.8.4 Network access control

**3.8.4.1** *The IT department is responsible for ensuring that network access is granted in accordance with access policy.*

**3.8.4.2** *Users should only have access to the services they are authorized for.*

**3.8.4.3** *The access to privileged accounts and sensitive areas should be restricted.*

**3.8.4.4** *Users should be prevented from accessing unauthorized information.*

### 3.8.5 Mobile equipment and remote workplaces

**3.8.5.1** *Remote access to <X University>'s computer equipment and services is only permitted if the security policy has been read and understood and the IT regulations signed.*

**3.8.5.2** *Remote access to <X University>'s network may only take place through security solutions approved by the IT department.*

**3.8.5.3** *Mobile units should be protected using adequate security measures.*

**3.8.5.4** *Information classified as sensitive must be encrypted if stored on portable media, such as memory sticks, PDAs, DVDs and cell phones. [The use of cryptography may be subject to local legislation.]*

## 3.9 Information systems acquisition, development and maintenance

### 3.9.1 Security requirements for information systems

**3.9.1.1** *Definitions of operational requirements for new systems or enhancements to existing systems must contain security requirements.*

### 3.9.2 Cryptographic controls

**3.9.2.1** *Guidelines for administration and use of encryption for protecting information should be in place.*

### 3.9.3 Security of system files

**3.9.3.1** *All changes to production environments should comply with existing routines.*

**3.9.3.2** *The implementation of changes to the production environment should be controlled by formal procedures for change management, in order to minimize the risk of damaged information or information systems.*

### 3.9.4 Security in development and maintenance

**3.9.4.1** *Systems developed for or by <X University> must satisfy definite security requirements, including data verification, securing the code before being put in production, and use of encryption.*

**3.9.4.2** *All software should be thoroughly tested and formally accepted by the system owner and the IT department before being transferred to the production environment.*

### 3.9.5 Risk assessment

**3.9.5.1** *Prior to new systems classified as "high" , or substantial changes in systems classified as "high" (see Table 1: System classification) are put in production, a risk assessment must be carried out.*

## 3.10 Information security incident management

### 3.10.1 Responsibility for reporting

**3.10.1.1** *All breaches of security, along with the use of information systems contrary to routines, should be treated as incidents.*

**3.10.1.2** *All employees are responsible for reporting breaches and possible breaches of security. Incidents should be reported to management or directly to the CSO.*

### 3.10.2 Measurements

**3.10.2.1** *Routines are to be developed for incident management and reporting. The routines should contain measures for preventing repetition as well as measures for minimizing the damage.*

**3.10.2.2** *The CSO should ensure that routines are in place for defining the cost of security incidents.*

### 3.10.3 Collection of evidence

**3.10.3.1** *The IT security manager should be familiar with simple routines for collecting evidence.*

## 3.11 Continuity planning

### 3.11.1 Continuity plan

**3.11.1.1** *A plan for continuity and contingencies covering critical and essential information systems and infrastructure should exist.*

**3.11.1.2** *The continuity plan(s) should be based on risk assessments focusing on operational risks.*

**3.11.1.3** *The continuity plan(s) should be consistent with <X University>'s overall contingencies and plans.*

**3.11.1.4** *The continuity plan(s) should be tested on a regular basis to ensure adequacy, and to ensure that management and employees understand the implementation.*

**3.11.1.5** *Production systems and other systems classified as "high" (see Table 1: System classification) should have backup solutions. The table below should be completed after carrying out a risk assessment and/or Business Impact Analysis (BIA). (This table is an example)*

| Criticality | Availability | Description |
|---|---|---|
| 3 – High | < 8 hours | The system may be unavailable for up to 8 hours |
| 2 - Medium | 24 hours | The system may be unavailable for up to 24 hours |
| 1 – Low | 3 days | The system may be unavailable for up to 3 days |

Table 1: System classification

## 3.12 Compliance

### 3.12.1 Compliance with legal requirements

#### 3.12.1.1 *<X> must comply with current laws, as well as other external guidelines, such as (but not limited to):*

**List of relevant national legislation**, e.g.:

- Act relating to working environment, working hours and employment protection, etc.
- Regulations relating to systematic health, environmental and safety activities in enterprises
- Act relating to the processing of personal data
- Act relating to civil servants, etc.
- Act relating to annual accounts, etc.
- Act relating to universities and university colleges
- Act relating to the right of access to documents held by public authorities and public undertakings
- Act relating to electronic signature
- Act relating to archives
- Regulations relating to fire preventing measures and supervision

**Other relevant references**

- Collective agreements

### 3.12.2 Safeguarding personal information according to the legal requirements

**3.12.2.1** *Insert relevant statements for your organization according to e.g. 95/46/EC and 2002/58/EC.*

### 3.12.3 Compliance with security policy

**3.12.3.1** *All employees must comply with the Information security policy and guidelines. Enforcement is the responsibility of line management. Students must comply with IT regulations.*

**3.12.3.2** *Employees and students should be aware that evidence from security incidents will be stored and may be handed over to law enforcement agencies following court orders.*
*[Must be updated to reflect national legislation.]*

### 3.12.4 Controls and audits

**3.12.4.1** *Audits should be planned and arranged with the involved parties in order to minimize the risk of disturbing the activities of <X University>.*

# 4 Governing documents for safety work

## 4.1 Purpose of governing documents

Governing documents for information security should contribute to a balanced level of measures with regards to the risks and requirements related to <X University>.

Documented requirements and guidelines should exist for information security based on up-to-date risk assessments. Systems and infrastructure should be covered by best practices for information security.

## 4.2 Document structure

**4.2.1.1** *<X University> has organized a document structure describing their security architecture in three levels. The structure for governing documents for information security work is as follows:*

*Level 1: Security policy*
**defining goals, purposes, responsibility and overall requirements. Additionally, it gives an overview over established governing documents regarding information security and why it is important.**
**This is the governing documentation.**

*Level 2: Overall guidelines and principles*
**for information security. This defines what must be done in order to comply with the established policy.**
**This is governing documentation.**

*Level 3: Standards and procedures*
**for information security. Contains details for how these guidelines and principles (level 2) should be implemented.**
**This is implementation and control documentation.**

# References

## Internal references

| Version | Date | Comment | Responsible |
|---|---|---|---|
| | | IT regulations at <X University> | |
| | | Strategy plan at < X University > | |
| | | Quality assurance system at < X University > | |
| | | IT strategy at < X University > | |
| | | Risk assessments | |
| | | Personnel policy | |
| | | Guidelines for the disposal of IT equipment | |
| | | Confidentiality agreement | |
| | | Role description CSO | |
| | | | |
| | | | |
| | | Other relevant IT related documents | |
| | | | |

## External references


**[ISO27001 ]** ISO 27001: 2005. Information security – Security techniques – Information security management systems – Requirements**.**

**[ISO27002 ]** ISO/IEC 27002: 2005 Information security – Security techniques – Code of practice for information security management .

**[ISO27005]** ISO/IEC 27005: 2008 Information security – Security techniques – Information security risk management .

**[OECD]** OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. http://www.oecd.org/dataoecd/16/5/15584616.pdf

**[BPD107]** Power Supply Requirements for ICT Rooms. Best Practice Document. http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs107.pdf

**[BPD108]** Ventilation and Cooling Requirements for ICT Rooms. Best Practice Document. http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs108.pdf