# Information Security Policy

UM

2013

# Colophon

*UM Information Security Policy, Version 2.1 (2013)*

Replaces UM Information Security Policy, Version 1.0 (2003)

Author: Bart van den Heuvel, CISO, ICTS

Adopted by the Maastricht University Executive Board d.d.: 17 June 2013
Adopted by the University Council d.d.: 25 September 2013

Version 2.1: tekstual alignment with Dutch version

The UM's Information Security Policy is based on the *Model Informatiebeveiligingsbeleid van het Hoger Onderwijs* [Model Information Security Policy for Higher Education], a product of the SURF Chief Information Officers Consultation Group and SURFibo.

# Table of contents

# 1 Introduction

Information security is generally defined as the initiation and application of a coherent set of measures aimed at ensuring that the institute's information services meet the quality requirements of availability, integrity and confidentiality.

The quality aspects:
- Availability: the extent to which information and functionalities are available to users at the right times;
- Integrity: the extent to which information and functionalities are correct;
- Confidentiality: the extent to which the access to information and functionalities is confined to those who are authorised to use them.[1]

The above also includes the controllability of the measures taken to guarantee these quality aspects.

Information security falls under the responsibility of the UM executive board. In the fields of research and education we see an ever greater dependence on information and computer systems, which may lead to new vulnerabilities and risks. For this reason, it is important to take appropriate security measures. A lack of information security can lead to unacceptable risks when it comes to providing education, doing research and managing the institute. Security incidents and infringements on these processes can lead to financial damage and damages to the institute's reputation.

It is the UM's ambition to use this policy document to take information security to a higher level in a structured manner. Therefor the aspects relating to governance, rules and regulations, the organisation of the information security function and the institute's information security policy will be clearly described and adopted, taking in account the way these different aspects interrelate.

## 1.1 Scope of the policy

This section addresses the scope and limits of the UM's information security policy and its applicability.

UM takes a broad view of information security. We realise that information security is closely related to and partially overlaps with other bordering policy areas, such as safety (environment, health and safety legislation), security (physical security) and business continuity. Attention is paid to these points of overlap at a strategic level, and alignment is sought with respect to both policy planning and content (see also Chapter 4).

The UM's information security policy pertains to all employees, students, guests, visitors and external relations (hiring/outsourcing), and covers all parts of the organisation. UM's information security policy also includes all equipment providing authorised access to the institute's network and other institutional ICT facilities.

Our information security policy focuses in particular on applications and information that fall under the responsibility of UM. This includes controlled information that is generated and managed by the institute itself, as well as uncontrolled information (e.g. statements made during discussions, on personal websites or on Social Media) for which the institute may ultimately be held responsible.

[1] Overbeek, Roos Lindgreen, Spruit: Informatiebeveiliging onder controle, ISBN 90-430-0289-5.

## 1.2 Purpose of the information security policy

The UM's information security policy aims to safeguard the continuity of business operations and minimise damage by preventing and reducing the impact of security incidents.

The specific objectives of the UM information security policy are as follows:

- Framework: the policy provides a framework for evaluating (future) information security measures against an official standard or best practice, and allocating the tasks, authorisations and responsibilities in the organisation.
- Standards: the ISO 27001[2] forms the basis for the organisation of the institute's security management. Measures are based on best practices in higher education and on ISO 27002.[3]
- Explicit: the principles and organisation of the institute's information security functions are documented and supported by the Executive Board, and hence by the entire organisation.
- Decisive: clear choices and active control of policy measures and their implementation.
- Compliance: the policy provides the basis for meeting legal requirements.

The proper structuring and aligning of the information security policy at UM adds demonstrably to the realisation of the institute's overarching objectives. These objectives include the provision of a high-quality education and research environment, which will contribute to the improvement of the quality of society as a whole. The UM environment should be a safe one, and satisfy the relevant legal requirements and regulations.

[2] NEN-ISO/IEC 27001: Information security management systems requirements.
[3] NEN-ISO/IEC 27002: Code of practice for information security management.

# 2 Policy principles for information security

## 2.1 Policy foundations and principles

Security management is organised as a process (ISMS: Information Security Management System). The planning and control cycle is based on ISO 27001 (Plan, Do, Check, Act), and includes the development and implementation of annual plans. Next, the results are evaluated and translated into new annual plans.

The following policy principles are applied at UM:

- Our philosophy is that we are an open institute that offers plenty of scope for initiative. This open environment characterises the institute's research in particular. The approach we take to ICT and information security is stricter, however. Staff and students are expected to behave 'decently' in terms of technology and attitude (responsibility). It is considered unacceptable to create unsafe situations – either intentionally or unintentionally – that may cause damage and/or hurt our reputation. For this reason, codes of conduct have been formulated and implemented.
- The institute's information security policy must comply with the relevant laws and regulations, in particular the Personal Data Protection Act (2001).
- Information security must safeguard the following aspects:
    - availability;
    - integrity;
    - confidentiality.

UM applies the following policy principles:

- Information security is a process responsibility: this means to say that the process managers (or system owners) are primarily accountable for safeguarding the information for which they are responsible (source processes or systems, such as SAP-HR HCM and SAP SLM, and related processes and systems, such as UMcard and EleUM). This principle includes what policy measures are chosen, and their implementation and enforcement.
- Information security is a line responsibility: this means to say that the line managers (directors/department heads) hold the main responsibility for the information security in their own Business unit/department. This principle includes what policy measures are chosen, and their implementation and enforcement.
- Information security is everyone's responsibility. Expectations regarding individuals: communicate to the staff, students, lecturers and others that an active contribution should be made to the security of digitalised systems and the information stored in these systems. This message is communicated in letters of appointment, during appraisal interviews, in the institute-wide code of conduct, during periodic awareness campaigns and so forth. The imposition of sanctions after violation of this code make it a tangible and credible one.
- Information security is a continuous process. Regular reverification of policies and audits: technological and organisational developments inside and outside the institute necessitate the periodic revision of policies and a reassessment of the security methods used. The audits allow for efficiency checks of the policy and the measures implemented (controllability). In terms of the frequency and maturity level of the audits, UM aims to keep in pace with the continuing developments in higher education – as specified by the SURFaudit framework[4]. Policy revisions are part of the PDCA cycle in the ISMS process.
- Ownership of information. The institute is the legal owner of the information that is produced under its responsibility, unless otherwise agreed, for example for research. The institute also manages information legally belonging (copyright) to third parties. Staff and students should be well-informed about the rules for using this type of information.
- Value of information. Everyone should realise the value of information and act accordingly. The value of information is determined by the damage that would be caused in the event of

[4] SURFaudit assumes (in 2012) at least a self-assessments every 2 years and an external audit every four years. A maturity model has been developed in accordance with the CMM model (0-5), with level 3 as the minimum level.

reduced availability, integrity and confidentiality. Classification of information can be useful in this respect – see below.
- When projects are being implemented, such as infrastructural changes or the purchase of new systems, information security is taken into account right from the beginning.

## 2.2 Information classification

All information at UM covered by this information security policy must be classified. The level of security that applies depends on the classification of the information.

The classification of information depends on the data in the information system and is determined based on risk analyses.
To achieve this purpose, UM has adopted classification guidelines[5] for a mandatory minimum (generic) risk analysis.
The following aspects are important for the classification of information:
a. Availability
b. Integrity
c. Confidentiality.
For all three aspects, UM applies the classifications of 'Standard', 'Sensitive' and 'Critical'.

The following classifications are distinguished with regard to the availability requirements:
- Standard (information is not vital): complete loss or unavailability of this type of information for more than one week causes no noticeable (measurable) damage to the interests of the institute, its employees or its clients;
- Sensitive (vital information): complete loss or unavailability of this type of information for more than 48 hours causes noticeable damage to the interests of the institute, its employees or its clients;
- Critical (extremely vital information): complete loss or unavailability of this type of information for more than 4 hours causes noticeable damage to the interests of the institute, its employees or its clients.

Other general characteristics, such as possible computer disruptions at a critical time, may also be a reason for moving information, systems or processes to a higher security classification.

The following categories are applied to confidentiality and integrity.

| Class | Basic principles |
|---|---|
| Standard (public information) | • All staff and students (i.e. everyone) has access to this information, for example, via the UM Intranet or the institute's general website.<br>• A selected group of people is authorised to revise this type of information. |
| Sensitive (internal, confidential information) | • Access is reserved for private persons or anyone within the institute (employee, student or researcher) with a particular role or who belongs to a particular group; access can be granted from both inside and outside the institute (internal and remote access). Examples are self-service information, class schedules, department intranet and research databases.<br>• A select group of people is authorised to revise this information. |
| Critical (strictly confidential information) | • It is explicitly stated who has what rights regarding access to and processing of this type of information and, also, from which workstations the information can be retrieved. Examples are course results and research databases with (special) personal details. |

In addition, certain other general characteristics, such as contractual agreements or susceptibility to fraud, may be a reason for moving information, systems or processes to a higher classification.

Which particular level of security will be suitable for certain types of information or information systems depends on the classification of the information processed in the system. The classification

[5] 2007: "Classification-guidelines UM"

has to be determined by or on behalf of the owner of the information or information system concerned.

The table below shows the security level that goes with the different classifications:

| Availability | |
|---|---|
| Standard | Basic protection |
| Sensitive | Basic protection + |
| Critical | Basic protection ++ |
| **Confidentiality** | |
| Standard | Basic protection |
| Sensitive | Basic protection + |
| Critical | Basic protection ++ |
| **Integrity** | |
| Standard | Basic protection |
| Sensitive | Basic protection + |
| Critical | Basic protection ++ |

Individual security measures are needed for information systems that require more than a basic level of protection. Thus, the 'basic protection +' level indicates a higher security level than basic protection. 'Basic protection ++' is the highest security level available at UM. UM has constructed a measures database[6], which specifies a number of standard measures (the baseline) and a set of additional security measures for sensitive and critical information and information systems.

[6] 2007: MIB-UM (Dutch).

# 3 Laws and regulations

## 3.1 Legal requirements

The relevant laws and regulations are addressed at UM as follows.

### 3.1.1 Higher Education and Research Act

UM has organised its processes for education and research in such a way that it ensures that e.g. information in the student administration system and student results are handled with care, and that the processes for handling information comply with the Higher Education and Research Act. In addition, integrity codes for scientific research and ICT staff are applied and adhered to.

### 3.1.2 Personal Data Protection Act

By means of its information security policy, UM has fulfilled the legal requirements (of accuracy and precision of information, and appropriate technical and organisational measures against loss and unlawful processing). UM has applied its information security measures in accordance with the Data Protection Authority guidelines for 'Protection of Personal Data' (Feb 2013). Compliance with the security measures means that the requirements of the Personal Data Protection Act are met.

### 3.1.3 Public Records Act

UM adheres to the laws of the Public Records Act and the Public Records Decree on how information should be recorded in digitalised documents, information systems, websites, etc. This is part of the annual external audit reports.

### 3.1.4 Copyright Act

UM does not distribute any original works without obtaining permission from the copyright holder. This also implies that UM discourages the use of software without proper licensing.

### 3.1.5 Telecommunications Act and net neutrality

The UM network is not a public network. This means that the Telecommunications Act and, in particular, the stipulations on netneutrality do not apply. UM only provides Internet access to its staff and students if this is needed to support their work or studies. In as far as UM offers Internet access to students in their private accommodation, it will apply net neutrality. The UM offers internet access to other legal persons within the UM buildings by means of independent public providers; in these cases, the Telecommunications Act does apply.

The measures taken by UM to comply with the privacy legislation are also sufficient to ensure the protection of users' privacy when accessing the internet via UM's Internet facilities.

### 3.1.6 Computer Crime Act

The Computer Crime Act focuses on the legal problem areas relating to computer usage. The act dictates that 'a certain level of security' must be met before anyone can be prosecuted for committing an offence against the educational institute and the possible indemnification of the institute's management.

Compliance with this information security policy and implementation of the basic measures at UM should ensure a level of information security that complies sufficiently with the Computer Crime Act.

## 3.2 Other guidelines and national agreements

As stated above, the UM information security policy is based on ISO 27001.

UM complies with the following guidelines and national agreements:

- Integrity codes for scientific research
- Studielink agreements
- SURFnet/SURFconext connection conditions.

In addition, UM strives to adhere to the general national agreements for the industry as much as possible.

# 4 Information security governance

The good, effective and responsible running of an organisation is often referred to as 'governance'. Governance comprises in particular the relationships with key stakeholders of the institute, such as the owners, employees, students, other clients and society as a whole. A good corporate governance policy safeguards the rights of all these stakeholders.

## 4.1 Alignment with related policy areas

Good governance also means to say that sufficient attention is paid to all sorts of risks, and how these risks mutually affect each other. At the strategic level, UM focuses not just on information security, but also on physical security, health and safety and business continuity. Coordinating and integrating these different domains is a prerequisite for good governance. Such close coordination is translated into practice by allowing the various aspects to run parallel in the budgetary planning and reporting cycles, which act as a tool for identifying and addressing mutual interference. Where appropriate and possible, alignment is also applied at the tactical and operational level, but only if it renders additional value.

This chapter focuses exclusively on IT governance and the positioning of information security within the IT domain.

## 4.2 Alignment with IT governance at the institute

This section describes how IT governance is organised at UM and who is responsible for what. It is important to distinguish between the directional or strategic, the steering or tactical and the operational levels. The labels applied to the different roles match those specified by the platform for information security (PvIB)[7] as closely as possible.

The Corporate Information Security Officer (CISO) is a role at the strategic (and tactical) level. Together with the ICT Director and the Chief Information Officer, the CISO informs and advises the Coordinating Directors' Board and, If necessary, also the Executive Board. (. The CISO monitors the uniformity within the institute and is responsible for the ISMS process.

The role of Information Security Manager is defined at the staff level of every faculty or department, and is assigned to the Information Manager. The Information Manager plays a role in translating the strategy into tactical (and operational) plans. The Information Manager works closely with the CISO (to ensure uniformity), the ICT representative of the business unit (DO-ICT member, tactical/operational), those responsible for processes and the technical platform owners.

At the operational level, the functional managers and local IT officers regularly consult each other (via the DO-ICT members). Attention is paid to the implementation of information security. The handling of emergency computer incidents is initiated and coordinated by UM-CERT.[8]

[7] Functies in de informatiebeveiliging. Platform voor Informatiebeveiliging (PvIB), 2006.
[8] UM's Computer Emergency Response Team: http://www.maastrichtuniversity.nl/um-cert.

Overview:

| Level | What? | Who? | Consultation | Documents |
|---|---|---|---|---|
| Directional | - Adopting IS strategy<br>- organising IS<br>- establishing IS planning and control<br>- Business continuity management | Executive Board/Coordinating Directors' Board, in casu IS portfolio holder, based on advice from CISO and ICT Director/CIO | - Executive Board/Coordinating Directors' Board adopt<br>- Strategic IS/ICT meeting (UMIO) advises<br>- Approval University Council if applicable | - IS policy plan<br>- Integrity Codes and codes of conduct<br>- Classification guidelines/basic principles<br>- Business continuity plan |
| Steering | IS Planning & Control<br>- preparing standards and methods for evaluating<br>- evaluating policy and measures<br>- supervising internal assessments and external audits | - System owner<br>- CISO<br>- Information Security Manager | - Tactical IS/ICT consultation (in UMIO) | - IS baseline (basic Measures)<br>- Classifications, risk analyses and audits<br>- Annual plan and report |
| Operational | - implementing IS measures<br>- recording and evaluating incidents<br>- communicating to end users | - Information Security Manager<br>- Functional manager<br>- ICTS operations (Service Desk) | - Operational IS meeting (in DO-ICT or in business unit)<br>- UM-CERT | - SLAs (security clause)<br>- Incident registration incl. evaluation<br>- Operational UM-CERT framework |

The funding for information security at UM is organised as follows.

General issues, such as developing an information security plan for the entire institute or an external audit, are covered by the central ICT budget. The costs of security measures for of information systems are covered within the budgets of the specific information systems. The costs of protecting work stations are part of the integral workplace costs.

UM-CERT too, is financed by operational ICT budgets (mainly ICTS Operations), because the tasks involved fall under the regular duties of the UM-CERT members. UM-CERT has a number of additional mandates, including a mandate for an emergency budget for support during serious, institute-wide incidents.

Awareness and training can include institute-wide awareness campaigns (centrally funded) and local information supply and training for specific applications or target groups (locally funded).

## 4.3 Information security documents

The phases of the management cycle that is used for other policy fields at UM also apply to information security: policy development, analysis, implementation of plans, execution, monitoring and evaluation.

UM has the following documents relating to information security:

1. The information security policy
   The UM's information security policy (this document) provides the foundation for the approach taken to information security. The information security policy lists requirements and principles, and the manner in which the general policy is translated into concrete measures. In order to ensure that the general information security policy is supported and adhered to by the organisation, it is promoted by the Executive Board (or by others on the board's behalf). The general information security policy is outlined by the Corporate Information Security Officer, after which is it approved by the Executive Board.

2. Classification guidelines and measures database (basic and additional level measures)
   The classification guidelines set the criteria for the security measure levels (Standard, Sensitive or Critical) to guard the aspects of availability, integrity and confidentiality. In addition, a number of basic security principles are set out in the guidelines.

   The measures database describes in detail the principles that need to be implemented to ensure a minimum level of information security (baseline) at the institute level, and the additional measures for information or systems that are classified as sensitive or critical.

   The actual measures are derived from the IS policy or from decisions taken in the tactical meeting. The basic measures must be implemented in the entire institute. The baseline is created by the Security Managers and approved by the Executive Board. When systems require a higher level of security because of their classification or an additional risk analysis, corresponding measures are taken in addition to the minimum measures.

3. Annual plan/report
   Each year, the Corporate Information Security Officer (CISO) supplies an annual report and an annual plan for the following year on behalf of the ICT Director, the Chief Information Officer (CIO) and the Operations Manager of the Executive Board. The basis for the annual report is formed by comparable annual reports and the plans drawn up by the Information Security Managers. The annual plan is partly based on the results of the periodic audits. It lists specific incidents, the results of risk analyses (including the measures implemented) and other initiatives that have taken place in the preceding twelve months. Such reports can be ratified in the managerial planning and control cycle. If needed, special attention is paid to decentralised systems.

4. Business continuity plan
   Business Continuity Management (BCM) is a label for the process of identifying potential threats to an organisation, and determining what the impact would be on the organisation's 'operation' if these threats were to materialise. The BCM's product consists of a coherent set of measures aimed at preventing, detecting, countering and correcting threats.

   The Business Continuity Plan is coordinated by the Business Continuity Manager (or the CISO) and partly developed by the process and system owners. The Coordinating Directors' Board formulates the plan following the advice of the ICT Director, the CIO, the Technical Services Director and the Finance Director.

5. Service level agreements
   A 'service level agreement' is an agreement between a supplier and a customer about the conditions under which a certain service is provided. This can pertain to either the internal or the external level. To illustrate, the ICT department has an SLA with external suppliers for support of the concern systems and with UM's internal customers ICT for services such as the Service Desk and email services. These contracts contain a standard section on information security that addresses the supplier's responsibilities.

6. Hiring and outsourcing contracts
   When hiring services and personnel from third parties, attention needs to be paid to the aspect of information security. For example, these hired employees must be informed that the

information security policy of the institute will also apply to them. The same goes for outsourcing. The general UM Purchasing Conditions for ICT usually apply as well.

7. Integrity codes and codes of conduct
   This consists of codes of conduct and guidelines for staff, students and others – whether or not it concerns specific target groups – regarding information security. The codes have been laid down by the Executive Board, with the approval or advice from the representative offices:
   - Acceptable Use Policies (AUPs), for safe usage of ICT facilities;
   - Integrity code and codes of conduct for ICT officers.

8. Policies
   Additional guidelines at the operational level, such as:
   - password policy;
   - basic workstation requirements (including BYOD guidelines);
   - policies for the configuration and management of servers and network components;
   - application of cryptographic tools;
   - specific user and management conditions;
   - policy for sanctions, e.g. disconnection of faulty servers and workstations;
   - code of conduct for safe email traffic and Internet use.

## 4.4 Audit, compliance and sanctions

At UM, the Corporate Information Security Officer (CISO) supervises the monitoring of the implementation of annual information security plans. The CISO cooperates closely in this with the internal auditor.

The external audit is conducted by independent accountants. This event is linked to the annual audit and is integrated with the regular planning and control cycle as much as possible. Furthermore industry-specific audits are performed, e.g. SURFaudit.

The findings of the internal and external audits form input for UM's new annual plans.

Compliance with the rules means that the daily practice of the security management process is supervised in general terms. Of interest here is that line managers take their responsibility and hold their employees accountable for any shortcomings. The Data Protection Officer[9] plays an important role in promoting compliance with the Personal Data Protection Act.

If compliance is seriously lacking, UM can sanction the responsible employees, within the framework of the collective labour agreement and the legal possibilities. Students may also be sanctioned, in line with the Higher Education Act.

## 4.5 Awareness and training

Policies and measures do not mean that information security risks can be wholly avoided. In practice, when things go wrong people are usually shown to be the main culprits. UM therefore constantly tries to alert people to information security risks, and promote safe and responsible behaviour. As part of its policy, regular awareness campaigns are organised for staff, students and guests. These campaigns can tie in with national campaigns in higher education, if possibly in coordination and conjunction with security campaigns for environment, health and safety. Increasing the awareness of the importance of information security is a task of both the (local) Information Security Managers and the CISO. Ultimately, the Executive Board is responsible.

[9] As of 2014, the institute is required to officially fulfil this role.

Methods are being implemented to anchor this sense of awareness in employees' career paths, for example, by making the evaluation of integrity codes and codes of conduct a standard point on the agenda of annual interviews.

## 4.6 Organisation of the information security function

To ensure that the information security process is well-structured and coordinated, a number of roles are highlighted that are assigned to officials in the existing UM organisation.

### 4.6.1 Executive Board

The Executive Board is ultimately responsible for the information security at UM, and outlines policies, codes of conduct, and classification guidelines based on the general information security principles. The Corporate Information Security Officer (CISO) is responsible for information security at a content level. It is the CISO's task to ensure the information security at the entire institute.

### 4.6.2 Portfolio holder for information security

A member of the Executive Board is appointed as the portfolio holder for information security. This person is responsible for information security at UM.

### 4.6.3 Corporate Information Security Officer

The Corporate Information Security Officer (CISO) is a role at the strategic (and tactical) level. The CISO advises the Coordinating Directors' Board together with the ICT Director and CIO (information management). If necessary, they also advise the Executive Board. The CISO guards the uniformity within the UM and the ISMS process.

### 4.6.4 Information Security Manager

The role of Information Security Manager is defined at the staff level of each business unit. At UM, this role is assigned to the Information Manager, who helps to translate the general strategy into tactical (and operational) plans. The Information Managers do this together with the CISO (so to ensure uniformity), and with the process and ICT service owners.

### 4.6.5 Process owner

Process owners are responsible for primary or support processes, such as purchase, HRM and education.

### 4.6.6 ICT service owner

The ICT service owner is responsible for ensuring that an application provides good support for a specific process. This means that the ICT owner ensures that the application continues to meet the needs and demands of users and that it complies with rules and regulations, both now and in the future. Of course, the application must also meet the information security policy rules and at least the basic measures.

### 4.6.7 Information architect

The information architect provides advice on specific information security measures in processes and systems and monitors the consistency of those measures.

#### 4.6.8 Line Manager

Compliance with the information security policy is a component of the overall business operation. Each Line Manager is responsible for:

- ensuring employees are aware of the security policy;
- monitoring compliance with the security policy by employees;
- periodically bringing the topic of information security to the attention in work meetings;
- being available as a point of contact for all staff about information security matters.

The Information Security Manager or CISO can support the Line Manager in these responsibilities.

#### 4.6.9 Data Protection Officer

The Personal Data Protection Officer monitors the implementation of and compliance with the Personal Data Protection Act at UM. The statutory duties and responsibilities of the Personal Data Protection Officer give this officer an independent position in the organisation.

#### 4.6.10 CERT Coordinator

The CERT Coordinator at UM is appointed by the ICTS Director at institutional level and operates under the director's directive. The CERT Coordinator chairs the UM-CERT team. The team has additional mandates, directly under the Executive Board portfolio holder, with powers to limit the functionality of computer systems, network segments or users (or user groups).

## 4.7 Consultations

Structured consultations are held at UM about information security at many different levels, with the aim of emphasising the coherence in the organisation of the information security function and ensuring that the information security initiatives and activities are aligned across the various components.

At the strategic level, the ICT Director/CIO, portfolio holder on the Executive Board and the Coordinating Directors' Board discuss governance and compliance, as well as objectives, the scope and ambitions with regard to information security. The Information Managers consultation, which is coordinated by the CIO, has an advisory role at the strategic level.

At the tactical level, the strategy is translated into plans, standards, evaluation methods, etc. These plans and instruments guide the actual implementation. The tactical consultations are organised per faculty or service by the director or Information Manager. Overarching tactical advice is provided by the ICT representatives of the business units in the DO-ICT consultation.

At the operational level, matters relating to the daily operation of security (implementation) are addressed. Overarching issues to do with information security are discussed in meetings (coordinated by ICTS) with the ICT representatives of the business units (DO-ICT). The 'users consultation', which is organised by all process or system owners, is a structured event at UM, where several operational issues can be addressed. Operational consultation also takes place at lower levels, if necessary in each different part of the organisation.

If possible all three types of consultation must be integrated into the existing consultation formats, with the same basic set-up if possible. Discussions at the strategic level, for example, do not only deal with information security, but also with other risks which can be encountered, such as financial, personnel and commercial threats.

# 5 Reporting and handling incidents

Incident management and registration relate to the reporting and handling of observed or suspected violations of information security by staff, students and researchers.

It is important to learn from incidents. Incident registration and periodic reports of incidents are an important part of a mature information security environment. The ICTS Service Desk at UM functions as a hotline and is publicly advertised as such.

Each business unit/department is responsible for identifying and reporting incidents and infringement of information security. The Line Manager, the local IT support staff or the end user should immediately report incidents and infringement to the hotline: ICTS Service Desk.

The ICTS Service Desk makes an initial assessment of all incoming incidents and other requests. If it concerns a security incident, the incident is assigned to the Security Group and initially classified as 'high risk'. Further analysis is conducted by the Security Group within the following four hours and either further action is taken (best effort) or the incident is placed in a lower classification level.

The incidents are dealt with and used as input for the incident reports, which are discussed during the operational consultation if necessary. Each quarter, an aggregated report is prepared, and discussed at tactical and strategic level. If certain trends are detected, these can be anticipated, for example, by taking additional measures or launching an awareness campaign.

## 5.1 Computer Emergency Response Team (CERT)

The purpose of the CERT at UM is to deal with major information security incidents and proposals for prevention at institute level. The CERT also deals with security incidents outside UM if the university's own employees or students are involved in any way. In cases such as these, UM will generally employ the services of SURFcert. SURFcert is in contact with other CERTs around the word.

The members of the CERT are appointed by the ICTS Director and operate under the director's directive.

The team has additional mandates, directly under the Executive Board portfolio holder. The CERT has the authority to limit the functionality of computer systems, network segments or users (or user groups).

At UM, the CERT has the following assignment:

- identifying and recording all security incidents, coordinating the response to and monitoring the resolution of problems that have led to incidents or resulted from the incidents (or providing support for this purpose);
- supplying information and making general recommendations to network administrators, system administrators, developers and end users;
- providing management reports to the ICTS Director and CIO (Information Management) about security incidents and making proposals for better prevention of or solutions for incidents.

The CERT provides the following services at UM:

- handling incoming emails;
- handling incoming phone calls;
- establishing and operating a hotline for all security incidents (ICTS Service Desk) and coordinating and monitoring adequate processes for handling these incidents (Security Solution Group). All stakeholders are informed about the accessibility of the CERT (times/resources);

- supplying information to IT users, developers and administrators about the prevention of incidents and current threats;
- providing advice about institute-wide security aspects;
- periodic preparation of management reports.

The CERT at UM treats all reports confidentially and only releases information about security incidents if necessary and relevant for resolving an incident.

The services provided by the CERT at UM are documented and endorsed by the Executive Board.