An Information Security Policy for the Faculty of Science (FNWI)

Spyridon Antakis, Henri Hambartsumyan

Radboud University of Nijmegen
Department of Computing & Information Sciences
6500 GL Nijmegen, The Netherlands , P.O. Box 9010
Email: {**s.antakis, h.hambartsumyan**}**@student.tue.nl**

November 9, 2009

Notice: This document represents only a draft version of Information Security Policy and it does not form the original policy of the FNWI.

Contents

1 Introduction

1.1 Preface

This document constitutes an *Information Security Policy Draft* for the Faculty of Science (FNWI). It aims to extend and strengthen the already established wide policy of University of Nijmegen, by clarifying some additional measures that will guarantee the protection of information resources inside the FNWI. At the same time, the ability of sharing information under the faculty's academic nature is preserved, but without neglecting the generally accepted information security principles of *confidentiality*, *integrity* and *availability*. The main purpose of this policy is to establish the responsibilities of each faculty member and define all the necessary actions that must be performed, in order to foresee, detect, prevent or mitigate any security risks, which can threaten the activities of the FWNI. In practice, the policy applies to anyone using faculty's information technology resources, including, students, staff, visitors, guests and third parties. The Faculty of Science is responsible to communicate the policy, procedures, guidelines and best practices to all of its members. In turn, every party involved is expected and required to review the policy, in order to be aware of his responsibility in protecting the information assets of the FNWI. Inside the policy, the measures are classified according to their criticality and their enforcement level is defined , as *must* or *should*. The procedures prefaced by *"must"* are mandatory as the system involved will be considered insecure without adherence. Guidelines and best practices are generally prefaced with *"should"* and are treated as mandatory, unless they are limited by functional or environmental considerations.

As in every policy design, the awareness about the organizational and management structure of the faculty is really important. The core business processes that are performed inside the FNWI and the all the physical location that belongs to the faculty, constitute the key factor for building an adequate Information Security Policy. Therefore, before this document describes the details of the security policy, presents first to the reader a brief introduction with respect to the pre-mentioned characteristics. In this way, any reviewer of the policy will be able to comprehend in depth the needs of the faculty. concerning the security of information resources.

1.2 Organizational Structure

The Faculty of Science (FNWI) consists of **6 Research Institutes**, **4 Education Institutes**, **7 Research Facilities** and **11 Service Departments**. The following tables present the exact organizational structure of FNWI.

Research Institutes
1. Institute for Water and Wetland Research.
2. Institute for Molecules and Materials (IMM).
3. Institute for Mathematics, Astrophysics and Particle Physics (IMAPP).
4. Institute for Computing and Information Sciences (ICIS).
5. Institute for Science, Innovation and Society (ISIS).
6. Institute for Molecular Life Sciences (NCMLS) - "Affiliated".

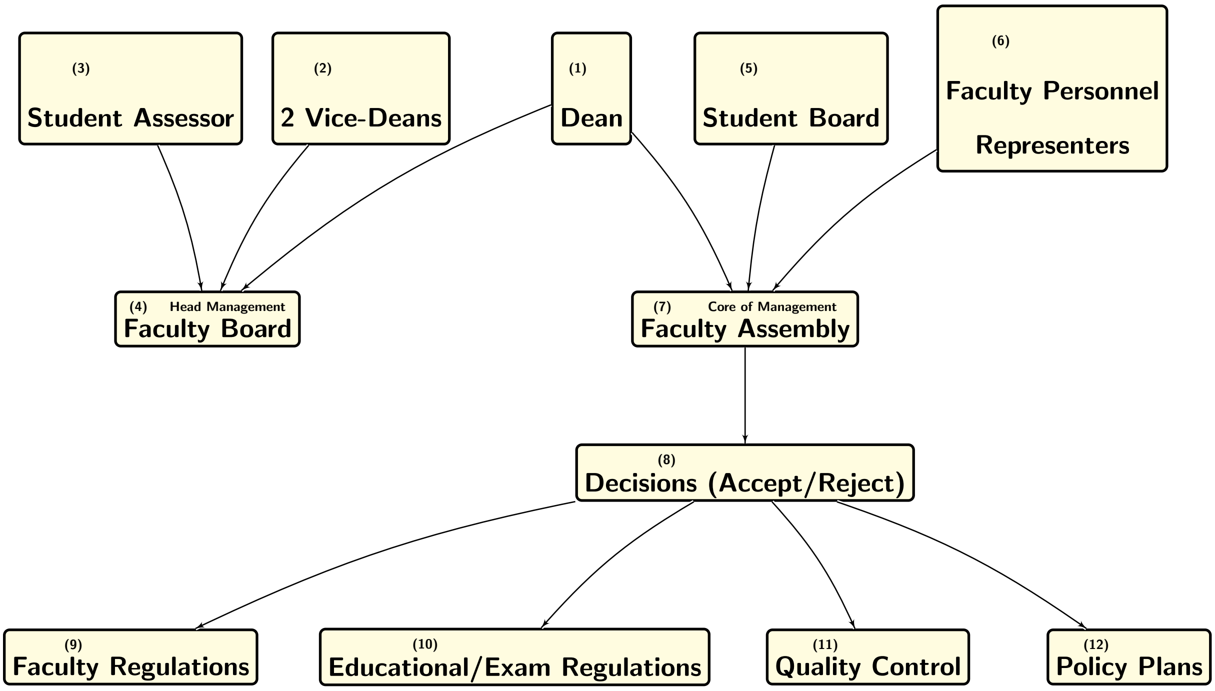
Educational Institutes
1. Institute of Life Sciences.
2. Institute of Mathematics, Physics and Astronomy (WiNSt).
3. Institute of Molecular Science (OMW).
4. Institute of Informatics and Information Management (III).

Research Facilities
1. Botanical and Experimental Garden.
2. Centre for Molecular and Biomolecular Informatics (CMBI).
3. General Instruments.
4. Goudsmit Pavilion.
5. High Field Magnet Laboratory (HFML).
6. Nanolab Nijmegen.
7. Phytotron.

Service Departments
1. Faculty Office.
2. C & CZ, Computer and Communications Department
3. Finance and Economic Affairs (FEZ).
4. Internal Affairs and Housing (IHZ).
5. Educational Affaires.
6. Human Resource Management.
7. Library of Science Library of Science.
8. Personnel Committee.
9. Techno Center (Technical Department).
10. EXO fulcrum.
11. Faculty Student Board.

1.3 Management Approval

In charge of any management approval inside the FNWI, is the Dean and the two Vice-Deans. More precisely, both are being advised by a Student-Assessor and all together constitute the Faculty Board. Every important decision is made from the Faculty Assembly, which is the meeting that Dean, Faculty's Personnel Representers and the Student Board participate.


(3) Student Assessor
(2) 2 Vice-Deans
(1) Dean
(5) Student Board
(6) Faculty Personnel Representers
(4) Head Management Faculty Board
(7) Core of Management Faculty Assembly
(8) Decisions (Accept/Reject)
(9) Faculty Regulations
(10) Educational/Exam Regulations
(11) Quality Control
(12) Policy Plans

In order the Dean to make any important decision about the FNWI, needs the permission of Faculty Assembly. Every action to change or finalize the faculty regulations, educational and exam regulations, the way of quality-control and policy-plans, must be approved by the Faculty Assembly or otherwise it cannot be performed. Finally, the Faculty Assembly is responsible to provide advice about reorganizations of the FNWI.

1.4 Definition of Information Security

In general, the operations of every University are based more or less on the same philosophy according the business activities. More precisely, the main business process of a University is to provide higher education at all kind of different levels. The *main objective* is to obtain the most adequate economical profits, by creating also a recognized reputation at both research and industry fields. In order this to happen, every University is separated in faculties with additional specific objectives, but without neglecting the pre-mentioned main objective.

The definition of Information Security for a University's Faculty, encloses a number of different processes. *Directly* or *Indirectly*, it involves processes related to business continuity and indicated a point of balance, in order all the business activities of the FWNI to be maintained at a desired level with respect to the Information Security requirements. In practice, information security constitutes an internal part of the overall business continuity process of FNWI, but also of the entire University Of Nijmegen. By taking a closure look at the FNWI business processes, we denote a number of different parties and facilities involved. The 6 research institutes, 4 education institutes, 7 research facilities and the 11 service departments contribute all together in a complex business procedure, which brings to the surface several *critical or not* points that should be identified and integrated to the information security management requirements of business continuity. In the following table, the most important core processes will be addressed, in order to have a better insight on the faculty's operation.

Core Processes
Registration Process
1. Personal information
2. Relevant documents
3. Tuition Fee
4. Scholarships
Network Infrastructure & Facilities Processes
1. Data handling
2. Services usage
3. Restrictions & Authorizations
4. Administration
Management Processes
1. Co-operation with third parties
2. Educational structure
3. Research subsidy
4. Business planning
Human Resources Processes
1. Professors
2. General staff
3. Expertise personnel
4. Third party employees
Co-related processes with other Faculties
1. Student accommodation
2. Common facilities
Other processes
1. Maintenance of faculties buildings & facilities
2. Operations related to faculty's library

1.5 Basic principles to follow

In accordance with the organizational structure described in 1.2, this policy defines an additional encapsulated security structure and performs a detailed evaluation with respect to all the critical information systems that involve FNWI. The university's baseline security is preserved and taken as the starting point (figure 1), however an individual baseline security is created for FNWI and the assets that belong to the faculty are treated separately. An individual risk assessment is conducted for every component and all the possible threats that can impact the business processes and the activities of FNWI, are identified with the intention to be controlled.

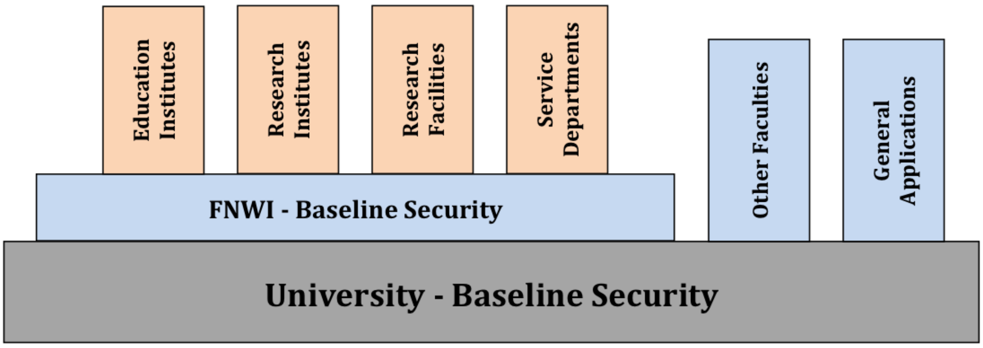


Figure 1: General security structure

2 Objective and Scope

2.1 In General

Information is a critical asset for the FNWI and it is comparable with other assets in a sense that there is a cost in obtaining it and a value in using it. Shared information is commonly used and loss or misuse can be sometimes costly or even illegal. The objective of this security policy draft is is to protect the information assets of FNWI and govern all aspects of hardware, software, communications and information. Faculty of Science is committed to protecting the *confidentiality*, *integrity*, and *availability* of information assets owned, leased, or entrusted to the faculty and thus also to the University. This document provides direction and support for information security in accordance with the general University requirements, however is focused on the relevant faculty operations. Security practices are designed to promote and encourage appropriate use of information assets, without any intention to prevent, prohibit, or inhibit the sanctioned use of information assets as required to meet the facultys core mission.

2.2 Confidentiality

All information hosted or created by FNWI are property of the faculty and as a transparency of the University of Nijmegen. As such, this information is solely used for related faculty duties or University purposes and any transfers or disclosures are restricted by a number of rules. The proper security standards are applied in order to prevent the inappropriate transfer of sensitive or confidential information. Release of information is strictly for job related functions and confidentiality is compromised when knowingly or inadvertently, information crosses the boundaries of job related activities.

2.3 Integrity

Integrity involves safeguarding the accuracy and completeness of information and processing methods. FNWI should be able to prevent deliberate or accidental, partial or complete, destruction, or unauthorized modification, of either physical assets or electronic data and all the faculty's members should comply with the relevant data-related legislation in those jurisdictions within which it operates.

2.4 Availability

The availability of information should be guaranteed by FNWI. Access to information will be granted as needed to all the faculty's members in order to support their required processes, functions and timelines. Usually, required availability varies depending on the needs of the process (i.e. constant, regular, periodical), however the faculty's mission must be to ensure availability at any form required.

3 Security Roles

The Information Security of FNWI resources is responsibility of all students, staff, visitors, guests and third parties involved. Every person handling information or using faculty's information systems is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at the FNWI. In practice, a number of security roles is required to be defined, in order the information security policy to be properly applied. In the following subsections, a short description of possible existing roles inside the faculty are given. However, note that the security roles should be managed dynamically according to the needs that faculty has, during an academic year.

3.1 Chief Information Officer (CIO)

FNWI should define a separate Chief Information Officer (CIO), which will be responsible for the faculty's policy. Supervision of the policy must be undertaken by the Faculty Assembly and the CIO. Implementation of the information security policy should be managed from the CIO and any other designated personnel in FNWI or University.

3.2 System Administrators

The responsibility for security of computing and communication systems rests with the system administrators who manage those systems. System Administrator, refers to the individual who is responsible for system and network support for computing devices in a local computing group. In some instances, this may be a single person while in other instances the responsibility may be shared by several individuals. If an administrator is not designated, the owner of a computer is considered the System Administrator. System Administrators will:

1. Try to protect the communication networks and computer systems for which they are responsible.
2. Try to employ FNWI recommended practice and guidelines where appropriate and practical.
3. Co-operate with FNWI or University in addressing security problems identified by network monitoring.
4. Address security vulnerabilities identified by FNWI scans deemed to be a significant risk to others.
5. Report significant computer security compromises to the CIO.
6. Guarantee that all computer resources must provide a notice before logon stating that the computer and network are solely for use of users authorized by FNWI computing and that any unauthorized access is prohibited and may result in prosecution.
7. Ensure that information, which by law is confidential, must be protected from unauthorized access or modification. Data, which is essential to critical functions, must be protected from loss, contamination, or destruction.

3.3 Head of Departments & Management

Heads of departments will be responsible for managing all the computing or communication devices connected to the FNWI network. In practice, they will have to designate an individual if other than the manager of the area, with the duties to create and maintain a current contact list of individuals who are responsible for the computer(s) for each location in the faculty. Moreover, Head of Department should be responsible to report on the Faculty Assembly, any critical security vulnerabilities that appear inside their department and propose possible solutions for each case.

3.4 FNWI Computing Department

A small independent Computing Department is advised to be created. This department will:

1. Prepare and publish security alerts, notices, recommendations and guidelines for network and system administrators.
2. Monitor backbone network traffic, as necessary and appropriate, for the detection of unauthorized activity and intrusion attempts.

3. When a security problem (or potential security problem) is identified, the department will seek the co-operation of the appropriate contacts for the systems and networks involved in order to resolve such problems. In the absence or unavailability of such individuals, computing department may need to act unilaterally to contain the problem, up to and including temporary isolation of systems or devices from the network, and notify the responsible system administrator when this is done.
4. Carry out and review the results of automated network-based security scans of systems and devices on faculty's networks in order to detect known vulnerabilities or compromised hosts.
5. When appropriate, computing department will inform the system administrators and department managers of the planned scan activity providing detailed information about the scans, including time of scan, originating machine and vulnerabilities that were tested. The security, operation or functionality of the scanned machines should not be endangered by the scan.
6. Report the results of scans that identify security vulnerabilities only to the system administrator contact responsible for those systems.
7. Report recurring vulnerabilities over multiple scans to the Departmental Head, and or CIO.
8. If identified security vulnerabilities, deemed to be a significant risk to others and which have been reported to the relevant system administrators, are not addressed in a timely manner, the department will take steps to disable network access to those systems and/or devices until the problems have been rectified.
9. Provide assistance and advice to system administrators to the extent possible with available resources.
10. Co-ordinate investigations into any alleged computer or network security compromises, incidents and/or problems.
11. Co-operate in the identification and prosecution of activities contrary to University policies and/or the law.

3.5 Students & Employees

All Students and Employees of FNWI are expected to be familiar with both FNWI and University of Nijmegen policy documents. The guidelines and procedures related to information and network security should be clear and understandable. Moreover, both students and employes are responsible for the protection of confidential and other FNWI related information entrusted to them. Therefore, they are advised to keep such information secure by using appropriately complex passwords when storing the information and use encryption to transmit the information when available. When systems change ownership, either through disposal or transfer, students and employees or their designates are expected to ensure that data entrusted to them is removed from the system before the change of ownership. Working with Computing Department, all students and employees are responsible for using systems that are secure and updateable and have active virus scanning software installed when available. Furthermore, they must report suspected computer security incidents, such as evidence of "hacking" and other forms of compromise, to the proper Computing Department personnel immediately. Finally, students and employees that administer their own systems, should have also the solely responsibility for the maintenance and support of these systems.

4 Approach

4.1 System inventory

FNWI involves several different information systems. In order to perform a good risk analysis and get a clear understanding of the implemented information systems including their relationships among each other, a system identification is needed. In practice, the organizational structure is used, as defined in section 1.2.

Achieving a complete list of information systems should be the responsibility of the *Computer and Communication Department*. The department must at all times have a complete list of all information systems used by the faculty. The main reason to assign this operation to the Computer and Communication Department, is due to fact that department should be actually responsible for implementing all systems used. Initially, it could be hard to identify all systems. However, once all systems are identified, the list should only be kept up to date when new information systems are taken into use or old systems are abandoned.

4.2 System owners

An information system should have an owner with clearly assigned responsibilities. Each system owner should maintain his system regarding also any security risks. The owner of each information system should be defined by the policy rules more precisely it is advised that the owner of a system is the director of the department that uses the system as part of its core business. For example, a HRM system is the core processes of the Human Resource department, so the director of this department is should be the owner of the HRM system, being responsible for this system.

If this is not possible or an information system is the ”core” of multiple departments (note that it has to be the core of at least one department), then one director should be chosen.

4.3 Risk assessments

A risk assessment should be conducted every academic year (depending on the available economical resources) to make sure that the security policy stays up to date, since the environment of the faculty is in a constant change. These changes can influence the risks, thereby influencing also the security of the system. The risk assessment process must include identification and evaluation of risks, risk impacts and recommendation to reduce risks.

For each information system a risk assessment should be performed by the owner and audited by a supervisor. This assessment should identify all the threats to the particular information system, the vulnerabilities of that system and the impact of threat manifestation. The result of each assessment should be a list of potential threats with a high risk (e.g. high impact × chance of occurence). For each high risk threat in this list, there should be a number of controls that will mitigate the threat to an acceptable level and reduce the impact of each risk after implementing the defined controls.

4.4 Implementing controls

Ensuring that the controls chosen while doing the risk assessment are really implemented, is as important as identifying risks and choosing controls. Without implementing controls, there is no point in identifying risks. There should be always someone responsible for implementing controls. The most appropriate person for this task is the person that is also responsible for the information system, of course this is only a recommendation. We do not demand that the director of some department should implement this controls himself. However, he should make sure that the right people implement the right controls, that there is money available for implementing and maintaining a control.

4.5 Reviewing information security

Just like with risk assessment, every aspect covered in this policy, including the policy itself, should be review every academic year. This review should be done by a qualified ISO auditor in co-operation with the faculty. This will ensure the high quality of the information security. The auditor must check if the systems are inventoried in the right way, if the risk assessment makes sense and is logical and if the right controls are properly chosen and implemented. This will assure the faculty that their information security policy is correct, is adhered to, is enforced and works as wished.

Of course, besides these official reviews, there should be at least every six months a review of how the information security policy impacts the security risks. If the goals that FNWI specifies, are achieved with the defined controls, then there is only need for maintenance of the controls. This can be considered as an extra evaluation of the implementation of the policy, which creates means to steer future development in the policy, as well as in choosing the controls.

If it turns out that the implemented controls are not as effective as they should be, there are two possible reasons. Either the existing controls are inappropriately chosen or the policy that supports the information security is not correct. In order to identify this kind of mistakes, there should be a review of the policy and if changes are required in the policy, these changes should be made the soonest possible. However, if there are any occurred implications due to the performed changes, then new approaches should be considered for proper control enforcement.

5 Baselines

5.1 Access Control

Faculty's critical or protected information assets should have restricted access based on operational and security requirements. Appropriate controls must be in place to safeguard unauthorized access to critical and protected information assets. This includes not only the primary operational copy of the information asset, but also data extracts and backup copies. Access to FNWI critical information assets and protected data may be provided only to those having a need for specific access in order to accomplish an authorized task and must be based on the principles of need-to-know and least privilege. Authentication controls must be implemented for access to FNWI critical information assets and protected data. Authentication credentials used for access to faculty's critical information assets and protected data must be unique to each individual and may not be shared unless authorized by appropriate University or FNWI management. FNWI should maintain a documented process for provisioning approved additions, changes, and terminations of access rights and reviewing access of existing account holders. Authorized users and their access privileges should be specified by the data owner, unless otherwise defined by University's of Nijmegen policy.

5.2 Granting Access to Third Party Service Providers

Third party service providers may be granted access to FNWI information assets only when they have a need for specific access in order to accomplish an authorized task. This access must be authorized by an appropriate FNWI or University's official authorized personnel and it should be based on the principles of need-to-know and least privilege. Access to FNWI information assets by third party service providers must not be allowed until it has been authorized, appropriate security controls have been implemented, and a contract/agreement has been signed defining the terms for access.

5.3 Network Security

FNWI must appropriately design and segment its networks based on risk, data classification, and access in order to secure its information assets. Each faculty and thus also FNWI must implement and regularly review a documented process for transmitting data over the University's network. This process must include the identification of critical information systems and protected data that traverses or resides on the university's network. FNWI processes for transmitting or storing critical and protected data must ensure confidentiality, integrity, and availability. FNWI members must only have direct access to the services that they have been specifically authorized to use. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, such as public or external areas that are outside the Faculty's security management and control.

5.4 Security Awareness

The security awareness program must provide an overview of FNWI information security policies, and help individuals recognize and appropriately respond to threats to faculty's information assets. The program must promote awareness of: a) information security policies, standards, procedures, and guidelines, b) potential threats against FNWI information assets and c) appropriate controls and procedures to protect the confidentiality, integrity, and availability of information assets. After receiving initial security awareness training, all faculty's member must receive follow-up awareness training annually to reflect changes in information security policy and standards.

5.5 Security Training

When necessary, the FNWI information security program must also provide or coordinate training for individuals whose job functions require special knowledge of security threats, vulnerabilities, and safeguards. This training must focus on expanding knowledge, skills, and abilities for individuals who are assigned information security responsibilities.

5.6 Systems Planning and Acceptance

To minimize the risk of systems failure, an advance planning and preparation are required to ensure the availability of adequate capacity and resources. Projections of future capacity requirements should be made, to reduce the risk of system overload. The operational requirements of new systems should be established, documented and tested prior to their acceptance and use.

5.7 Collection of Personal Information

In order to comply with Dutch laws and regulations, the FNWI may not collect personal information unless the need for it has been clearly established in advance. Where such information is collected:

1. The FNWI will use reasonable efforts to ensure that personal information is adequately protected from unauthorized disclosure.
2. The FNWI should store personal information when it is appropriate and relevant to the purpose for which it has been collected.

5.8 Access to Personal Information

Except as noted elsewhere in FNWI policy, information about individuals stored on faculty's information systems may only be accessed by:

1. The individual to whom the stored information applies or their designated representatives.
2. Authorized FNWI members with a valid FNWI-related business need to access, modify, or disclose that information.

5.9 Access to Electronic Data

Individuals who store personally identifiable information (e.g., names, student numbers, social security numbers, addresses) must use due diligence to prevent unauthorized access and disclosure of confidential, private, or sensitive information. Browsing, altering, or accessing electronic messages (e.g., email or text) or stored files in another users account, computer, or storage device (e.g., disks, USB drives) is prohibited, even when such accounts or files are not password protected, unless specifically authorized by the user for FNWI business reasons. However, this prohibition should not affect:

1. Authorized access by a network administrator, computer support technician, or departmental manager where such access is within the scope of that individuals job duties.
2. University's response to court orders.
3. University's response to a request pursuant to public record disclosure law

Finally, FNWI staff that who access protected data must sign a confidentiality agreement. This agreement must be regularly renewed.

5.10 Employment Requirements

As part of an effective security program, potential employees must be informed of their information protection obligations and their trustworthiness to handle protected information must be considered. Positions involving access to protected information and positions of trust must consider requirements for background checks. FNWI personnel procedures must address these elements.

5.11 Separation or Change of Employment

FNWI must implement procedures to revoke access upon termination, or when job duties no longer require a legitimate business reason for access, except where specifically permitted by University policy and by the data owner. Unless otherwise authorized, when an employee voluntarily or involuntarily separates from the University, information system privileges, including all internal, physical, and remote access, must be promptly disabled or removed. Procedures must be implemented to ensure proper disposition of electronic information resources upon termination. Electronic and paper files must be promptly reviewed by an appropriate manager to determine who will become the data steward of such files and identify appropriate methods to be used for handling the files. If any electronic information resources are subject to a litigation hold, the faculty must ensure preservation of relevant information before final disposition of electronic information resources. Moreover, FNWI must verify that items granting physical access such as keys and access cards are collected from the exiting employee. Any access list that grants the exiting employee physical access to a secured campus limited-access area must be updated appropriately to reflect the change in employment status. Information system privileges retained after separation from the University must be documented and authorized by an appropriate FNWI personnel.

5.12 Monitoring Systems and Information System Logs

FNWI systems should be monitored to detect deviation from access control procedures and record system events to provide evidence in case of security incidents. Moreover, it must implement logging and monitoring controls on appropriate information systems and network resources. Activity records created by logging and monitoring controls must be reviewed regularly. Server administrators are required to regularly scan, remediate, and report un-remediated vulnerabilities to the system owner or application administrator within a prescribed timeframe. The risk level of a system determines the frequency at which logs must be reviewed. FNWI systems must complete a periodic, but not less than annual, risk assessment to ensure they follow the appropriate monitoring requirements.

5.13 Physical Security

Faculty must identify physical areas that must be protected from unauthorized physical access. Such areas would include data centers and other locations on the campus where critical or protected assets are stored. FNWI must protect these areas from unauthorized physical access while ensuring that authorized users have appropriate access. FNWI information assets stored in public and non-public access areas must be physically secured to prevent theft, tampering, or damage. The level of protection provided must be commensurate with that of identifiable risks. FNWI must document physical access to limited-access areas and review these access rights annually.

5.14 Malicious Software Protection

FNWI must have procedures in place to effectively detect, prevent, and report malicious software. Electronic data received from untrusted sources must be checked for malicious software prior to being placed on a faculty's network or information system.

5.15 External Facilities Management

The use of an external contractor to manage information processing facilities may introduce potential security exposures, such as the possibility of compromise, damage, or loss of data at the contractors site. Prior to using external facilities management services, the risks must be identified and appropriate controls agreed with the contractor, and incorporated into the contract. Particular issues that should be addressed include: identifying sensitive or critical applications better retained in-house, obtaining the approval of business application owners, implications for business continuity plans, security standards to be specified, and the process for measuring compliance, allocation of specific responsibilities and procedures to effectively monitor all relevant security activities, and responsibilities and procedures for reporting and handling security incidents.

5.16 Publicly Available Systems

Information on a publicly available system, e.g. information on a Web server accessible via the Internet, may need to comply with laws, rules and regulations in the jurisdiction in which the system is located or where trade is taking place. There must be a formal authorization process before information is made publicly available and the integrity of such information must be protected to prevent unauthorized modification. Software, data and other information requiring a high level of integrity, made available on a publicly available system, should be protected by appropriate mechanisms, e.g. digital signatures. Electronic publishing systems, especially those that permit feedback and direct entering of information, should be carefully controlled so that: information is obtained in compliance with any information protection legislation, information input to and processed by, the publishing system will be processed completely and accurately in a timely manner, sensitive information will be protected during the collection process and when stored, and access to the publishing

5.17 Mobile Computing

Formal procedures must be in place and appropriate controls must be adopted to protect against the risks of working with mobile computing facilities, in particular in unprotected environments. For example, such procedures should include the requirements for: *physical protection*, *access controls*, *cryptographic techniques*, *back-ups*, and *virus protection.* Procedures should also include rules and advice on connecting mobile facilities to networks and guidance on the use of these facilities in public places. Care should be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the faculty's premises. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities, e.g. using cryptographic techniques. It is important that when such facilities are used in public places care is taken to avoid the risk of overlooking by unauthorized persons. Procedures against malicious software should be in place and be kept up to date. Equipment should be available to enable the quick and easy back-up of information. These back-ups should be given adequate protection against, e.g., theft or loss of information. Suitable protection should be given to the use of mobile facilities connected to networks. Remote access to business information across public network using mobile computing facilities should only take place after successful identification and authentication and with suitable access control mechanisms in place. Equipment carrying important, sensitive and/or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the equipment.

5.18 Management of Removable Computer Media

Appropriate operating procedures must be established to protect documents, computer media (tapes, disks, cassettes, etc.), input/output data, and system documentation from damage, theft and unauthorized access. The following procedures should be followed: If no longer required, the previous contents of any re-usable media that are to be removed from the faculty should be erased. Authorization should be required for all media removed from the FNWI and a record of all such removals maintained. All media should be stored in a safe, secure environment, in accordance with manufacturers specifications. All procedures and authorization levels should be clearly documented.

5.19 Encryption

Encryption should be applied to protect the confidentiality of sensitive or critical information. Based on a risk assessment, the required level of protection should be identified taking into account the type and quality of the encryption algorithm used and the length of cryptographic keys to be used. Specialist advice should be sought to identify the appropriate level of protection, to select suitable products that will provide the required protection and the implementation of a secure system of key management. In addition, legal advice may need to be sought regarding the laws and regulations that might apply to the universitys intended use of encryption. Procedures for the use of cryptographic controls for the protection of information must be developed and followed. Such procedures are necessary to maximize benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use.

5.20 Segregation of Duties

Duties and areas of responsibility must be segregated between the FNWI employees, in order to reduce opportunities for unauthorized modification or misuse of information or services. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision must be implemented. It is important that security audit remains independent. Care should be taken that no single person can perpetrate fraud in areas of single responsibility without being detected. The initiation of an event should be separated from its authorization.

5.21 Firewalls

FNWI firewalls functionality must be documented and detail how they manage security policy as applied to network traffic and how they maintain internal security. System documentation must be detailed and follow also the University's policy guidelines.

5.22 Disposal of Media

Faculty's media containing sensitive information should be stored and disposed of securely and safely, e.g. by incineration or shredding or emptied of information for use by another application within the University. The following list identifies items that might require secure disposal:

1. paper documents
2. output reports
3. program listings
4. removable disks
5. optical storage media
6. system documentation

In practice, it would be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items. Disposal of sensitive items should be logged where possible in order to maintain an audit trail. Disposal of certain hardware must conform with University's policy.

5.23 Exchanges of Information and Software

Exchanges of information and software between faculty's departments should be controlled and should be compliant with any relevant legislation. Exchanges should be carried out on the basis of agreements. Procedures and standards to protect information and media in transit must be established. The business and security implications associated with electronic data interchange, electronic commerce and electronic mail and the requirements for controls should be considered. Agreements, some of which must be formal, must be established for the electronic or manual exchange of information and software. The security content of such an agreement should reflect the sensitivity of the business information involved.

5.24 Business Continuity and Disaster Recovery

An information security program needs to support the maintenance and potential restoration of operations through both minor and catastrophic disruptions. FNWI must ensure that its critical information assets can, in the case of a catastrophic event, continue to operate and be appropriately accessible to users. The faculty must maintain an ongoing program that ensures the continuity of essential functions and operations following a catastrophic event. Of course, the program should always be in compliance with the University's policy.

Control	**Effectiveness**	**Cost**
Access Control	High	Medium
Granting Access to Third Party Service Providers	High	Medium
Network Security	High	High
Security Awareness	High	Low
Security Training	High	Medium
Systems Planning and Acceptance	Medium	High
Collection of Personal Information	High	Low
Access to Personal Information	Medium	Medium
Access to Electronic Data	High	Low
Employment Requirements	High	Low
Separation or Change of Employment	High	Low
Monitoring Systems and Information System Logs	Medium	Medium
Physical Security	Medium	High
Malicious Software Protection	High	Medium
External Facilities Management	Medium	High
Publicly Available Systems	Low	High
Mobile Computing	Medium	Medium
Management of Removable Computer Media	High	Medium
Encryption	High	Low
Segregation of Duties	Medium	Low
Firewalls	Medium	Low
Disposal of Media	Medium	Low
Exchanges of Information and Software	High	Medium
Business Continuity and Disaster Recovery	High	High

6 Appendix I

Inventory of Information Systems

Each Information System that is implemented and used within the FNWI has a designated Owner. In practice, the owner of an Information System is responsible for: i) ensuring that accurate and thorough risk assessments are conducted and documented at appropriate points in the lifecycle of the system, ii) beginning prior to the system's implementation, and that the findings are applied to the effective management of risks over the entire life of the system, iii) ensuring that appropriate system-specific policies, procedures and safeguards are developed and implemented, to comply with all applicable FNWI and University's policies and all applicable laws and regulations and iv) designating a system administrator for each system. All research institutes and research facilities should have one central system with all the knowledge, contacts and information concerning the performed research. Of course, there is access control inside this information system to ensure the confidentiality and integrity of the information in the systems. The educational institutes all have the same goal, they aim to learn new students core competencies concerning their study. Of course, they're supported by information systems. In this context, the information system used is primarily*blackboard.* Since *Blackboard* is an information system used university wide, the management and responsibility of blackboard is taken care at university level and not at faculty level. The most interesting parts, with respect to information systems, are the service departments. In the following table, the most important information systems used by these departments are presented. Note that these systems can overlap over departments and that there are some generic information systems used by all departements of the FNWI, systems like email, internal telephony, external telephony, document management. These basic systems which are used by the whole university are under direct management of the university and not in the management of a faculty. For this reason, these system are outside the scope of this document.

Important Information Systems & Owners	
Information System	***Owner***
1. Faculty Office - Customer Relatiosnhip Management (CRM)	**Faculty Board**
2. C & CZ, Computer and Communications Department - Windows Active Directory Domain Services - Customer Relatiosnhip Management (CRM)	**Computing Department** (if exists) & **Head of Computer and Communication Department**
3. Finance and Economic Affairs (FEZ) - Billing System - Customer Relatiosnhip Management (CRM) - Enterprise Resource Management (ERP)	**Director of University's Financial Department** & **Dean**

4. Internal Affairs and Housing (IHZ) - Billing System - Human Resource Management (HRM) - Enterprise Resource Management (ERP) - Educational Affaires	**Director of University's Human Resource Department**
5. Techno Center (Technical Department) - Customer Relatiosnhip Management (CRM)	**Director of Technical Department** &
6. Library of Science - A library information system	**Director of University's Central Library** & **Director of the Faculty**
7. EXO fulcrum	**Director of the Faculty**
8. Laboratories of Research/ Educational Institutes	**Director of each Institute**
9. FSR Student	**Student Board**

7 Appendix II

Classification of Confidentiality

Unintended or Unauthorised Disclosure of Information					
Reference	**Question**	**Impact**	**Impact**	**Impact**	**Explanation**
V01	How privacy sensitive is the information?	Public	Basic (membership, subscription related, employee related)	High (medical, financial, sexual inclination)	
V02	How much time will be lost to recover from a leak	<1 day	1 - 3 days	>3 days	
V03	What will be the reputation loss if confidentiality is compromised?	Low (No real or just a little loss)	Moderate (Quite some loss)	High (Probably the end of business)	
V04	How much confidential data does the system contain	Only public	Some confidential data	A lot of confidential data	
V05	Are there enough measurements to prevent a breach	A lot / All public data	Enough	No	
Result	**Summary**	**Low**	**Medium**	**High**	
V	In summary, taking into account the ratings noted above and any other consequences, what is the most serious damage which would arise from unintended or unauthorized disclosure of Information?				

Classification of Integrity

Error or Manipulation in Information - Perpetrate or Conceal Fraud					
Reference	**Question**	**Impact**	**Impact**	**Impact**	**Explanation**
I01	Financial damage arising from unauthorized changes to information.	< 2.500 EUR	Between 2.00 EUR and 25.000 EUR	> 50.000 EUR	
I02	For how much percent of the information is integrity important	0-30%	30-60%	60-100%	
I03	For what part of the information will recovery of data be possible	All	Partial	Practically none	
I04	Possible wrong actions/decisions based on incorrect data	None	Some	A lot	
I05	What will be the reputation loss if confidentiality is compromised?	Low (No real or just a little loss)	Moderate (Quite some loss)	High (Probably the end of business)	
Result	**Summary**	**Low**	**Medium**	**High**	
I	In summary, taking into account the ratings noted above and any other consequences, what is the most serious damage through errors in or unauthorized changes to information?				

Classification of Availability

Prolonged Outage of the Application					
Reference	**Question**	**Duration**	**Duration**	**Duration**	**Explanation**
B01	How long can the system be unavailable until substantial financial damage (25k) occurs?	> 1 day	< 1 day	< 4 hours	
B02	Is manual processing possible	Yes	For 1-2 days	No	
B03	How much percent of the personnel cannot function if the system is unavailable	0-30%	30-60%	60-100%	
B04	After what downtime will important management decisions suffer substantially	> 1 day	< 1 day	< 4 hours	
B05	After how much time will the organization loose reputation due to unavailability of the system	> 1 week	1 - 7 days	< 1 day	
Result	**Summary**	**Low**	**Medium**	**High**	
B	In summary, what is the most serious damage which would arise from an outage of the application at worst possible time?				
	What is the critical timescale for recovery of this application?				