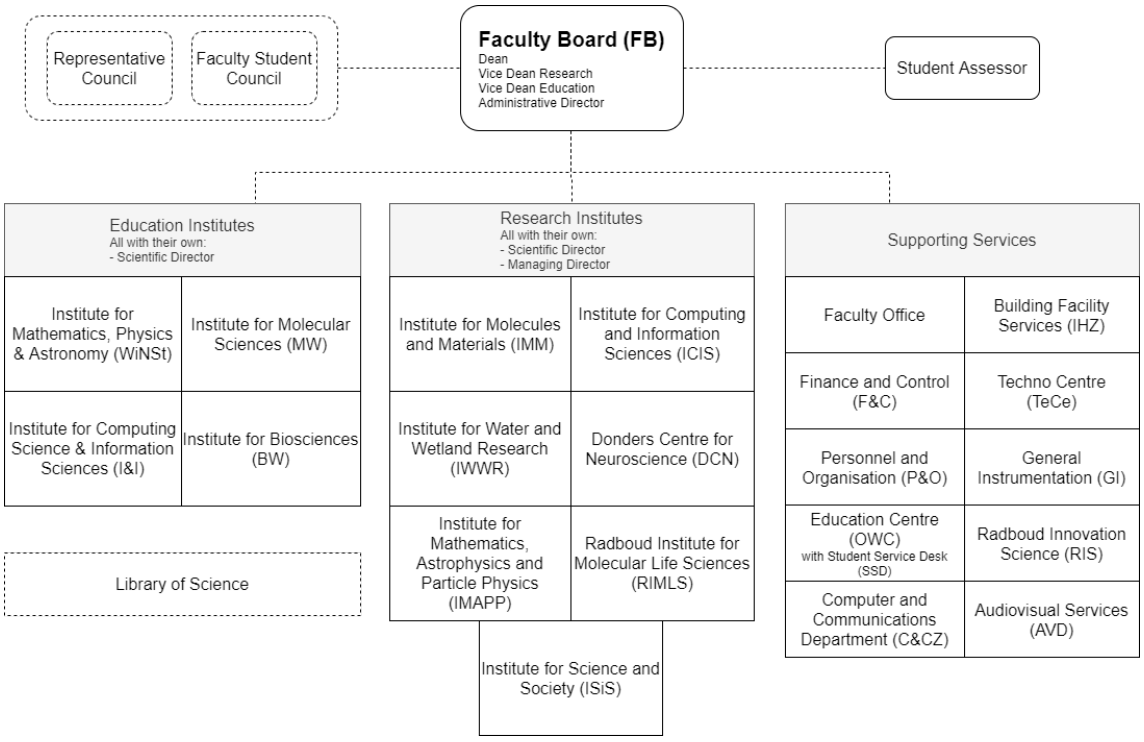
Information Security Policy - Faculty of Science

Casini Lorenzo Tommasini Martino

December 17, 2020

1 Introduction

The awareness about the organization and structure of the Faculty of Science (FNWI) is fundamental when writing the information security policy, to better understand its details.
The Faculty of Science has 7 research institutes and 4 educational institutes. The faculty also offers 10 supporting departments to provide aid to education, research and management.



As an educational institution, the faculty's core businesses are teaching and research. These need to provide a substantial economic income, as well as support and improve the faculty's reputation. In order to support this structure, the FNWI relies on the Service Departments which, in addition to their specific responsibilities, are in charge to handle and enforce internal policies and eventually advice the Faculty Board on matters related to their expertise. To properly address the faculty's core businesses, the following processes are carried out within the FNWI:

- Enrolment to faculty and courses;
- Hiring professors and general personnel;

- Definition of educational goals and study plan structures;
- Financial matters of faculty (e.g. student fees, projects funding and staff wages);
- Support to research organisations and activities;
- IT infrastructure and information handling;
- Library related matters.

The Faculty of Science is subjected to the security policy of the Radboud University (RU), as a faculty within it. Changes in the latter may consequently produce changes in the FNWI security policy. It is responsibility of Chief Information Security Officer (CISO) of the faculty to start a review of the FNWI security policy.
The FNWI depends on the services provided by RU or other third-parties to address the specific needs of the faculty. All specific services required by the Institutes or the research facilities are directly handled by the faculty. All other services not directly related to the faculty, such as cleaning, teaching platforms and devices to support the education are provided by RU. The third-parties involved in such processes are handled by RU as well.

2 Definition of information security

The ISO 27000 Information Security Management Systems (ISMS) standard states that Information Security is the "Preservation of confidentiality, integrity and availability (CIA) of information" which are defined as follows:

Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes
Integrity	The property of accuracy and completeness
Availability	The property of being accessible and usable upon demand by an authorised entity

In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved. A system can be defined as critical or non critical based on these CIA indicators.

The Information Security Standard ISO 27001 is the primary reference for designing and implementing information security within FNWI.

A large amount of sensible data is handled by FNWI, as processes require confidential or personal data to carry out their functions. Student data is collected and handled in the registration process, stored and managed during its whole educational path. The same applies to other processes such as the hiring process, all the financial matters of the faculty and the data needed and produced by the research infrastructures of FNWI. To allow a correct processing of such data, the IT infrastructure is expected to provide confidentiality by design.

Integrity is key to all processes that have to cope with confidentiality, but also to processes that expect high level of precision in data, such as financial, research and all educational activities.

Availability is especially important in educational processes. This applies to both digital and physical access to information, thus involving the reachability of online services provided by the IT infrastructure of the FNWI, as well as the availability of data in the library for educational and research purposes.

The IT department of the faculty is then expected to guarantee also for the integrity and availability of data. In addition, it should also provide a certain degree of non-repudiation and

reliability for the processes in which it is involved in order to be able to prevent and mitigate possible incidents or to recover and investigate the matter, should anything happen.

Authenticity of data should be a responsibility of the ICT department as long as data is stored and transmitted over the faculty's IT infrastructure.

Finally all involved parties in the above mentioned process are considered accountable for the data they consume or process based on the responsibility defined by this policy.

3 Management approval

The Faculty Board is in charge of governing and managing the faculty with regard to the quality of education and research. It consists of a Dean, two Vice-Deans and an Administrative Director; it is advised by a Student Assessor and assisted by a Secretary. Another management corp is the Faculty Assembly, the meeting in which the Dean, the Representative Council and the Faculty Student Council take decisions regarding faculty, educational and exam regulations, quality control and policy plans. The Dean needs the permission of the Faculty Assembly to change or finalise the above processes. The Faculty Assembly also gives advice about reorganisations of FNWI and appointing of professors.
The information security policy here described is reviewed by the Faculty Board and needs to be explicitly approved by the Faculty Assembly. The CISO of FNWI is responsible for the information security policy and, together with the Faculty Board, needs to review the policy in case of incidents or once significant changes are applied to the organisation, to the security objectives or to the business processes. The CISO of FNWI needs to guarantee the continuing suitability, adequacy and effectiveness of the policy. The security policy is also reviewed at the end of each academic year.
If adjustments on the policy are introduced, the document is again subjected to the approval of the Faculty Assembly. The Faculty Board is responsible for the enforcement of the policy.

4 Security objectives

As a faculty of the Radboud University, the main goal of FNWI is to provide valuable education to students. Great attention is given to the protection of students', employees' and third-party's intellectual property and privacy, as personal data is handled, transferred and consumed by faculty's processes. FNWI needs to ensure full commitment to the continuous improvement of the aspects concerning confidentiality, integrity and availability of information systems.

4.1 Confidentiality

Personal data or confidential information are only disclosed and transferred for RU related functions. Any disclosure of such information outside of the RU sphere is considered as a serious act and the Faculty Board is appointed to take actions against the transgressor. When confidential information are leaked, be it voluntarily, inadvertently or maliciously, the CISO is committed to investigate the causes and means of the perpetration and to further improve the current measures if needed.

4.2 Integrity

FNWI guarantees the integrity of information and systems hosted and handled by the faculty. All members of the faculty, ranging from Faculty Board to faculty's guests, ensure the accuracy and trustworthiness of the information transferred as well as the appropriate use of the provided devices and tools. Recovery procedures should allow the FNWI to recover possible damage or disruption of data.

4.3 Availability

FNWI guarantees the availability of information and services provided. The FNWI implements the necessary measures to avoid denial of service caused by nature or human threats (both intentional or unintentional).

4.4 Responsibility

FNWI is responsible of the data shared with third-party systems. As the intervention of a third-party in the faculty's processes and matters poses potential additional threats to the confidentiality, integrity and availability of information systems, the stipulated contracts must have a clear definition of obligations and responsibilities of the involved parties. The Faculty Board is appointed to request third-parties an annual report of the activities inherent the faculty and evaluate if any additional threats could be identified that were not part of the current policy or in the contract. The review of such documents is conducted by the CISO of FNWI and a final evaluation is done together with the Faculty Board. The conclusive decision shall not pose a risk to the confidentiality, integrity or availability of the FNWI systems and information.

4.5 Security objective renewal

The security objectives of FNWI may change over the time. The CISO of the FNWI is in charge of updating these to guarantee their appropriateness. The Faculty Board is appointed to communicate the security objectives to all students, employees and guests of FNWI as well as relevant third-parties.

4.6 Laws, Policies and Contracts

The security policy adheres to the Netherlands' laws of Data Protection, as well as the GDPR, and laws of Security of Information Systems. The security policy is build on top of the security policy of RU, in accordance with the requirements of the University. The faculty is also subjected to the same regulations, legislation and contracts mentioned in RU's policy.

5 Scope

The security policy applies to all the students, employees and guests of the FNWI as well as all networks, information and systems under the responsibility of the FNWI. Third-parties, which manage FNWI's data and use the services offered by FNWI, are also comprised in the scope. All assets, facilities and information within the physical or digital space of FNWI are subjected to the policy. The policy also applies to whoever interacts with FNWI's information or properties, regardless of their physical location (i.e. documents, laptops, mobile devices or any other intellectual property or transportable object property of the FNWI). Whatever falls under this scope needs to adhere to the security policy of RU as well.

6 Approach

6.1 Baselines

The FNWI's Baselines are developed following the ISO 27002 standards, see *Appendix I: Baselines*. They identify a series of controls that need to be implemented in all the systems of the faculty, be them critical or not.
The Baselines are implemented on top of the Baselines implemented by RU.

6.2 Information system inventory

In each of the identified core processes, all the information system currently in use should be inventoried down to its components according to the desired level of granularity requested by faculty. It is important to capture this information in detail to have a clear insight of all the assets. This process will facilitate the following implementation and management of all the security aspects of the whole system. In case of future changes to the system (e.g. additional equipment, replacement or disposal of existing ones), it is only needed to update the inventory accordingly.

6.3 Information system ownership

Each of the identified piece of information system in the created inventory should be assigned to an owner. The owner should be identified in a person related to the process in which the system is related, which is usually identified in the responsible for that business process. The owner is responsible for the security of the information system and for the application and communication of the controls and procedures for data handling as described in the Information Security policy. It is their responsibility to communicate to relevant parties any planned and unplanned changes in the piece of information system, as well as coordinate in case of damages, failures or intrusions. The owner is also responsible for the continuous verification that the controls and procedures are still actual and in place, and, in case, notify the CISO about needed updates or newly identified threats. Tasks can be delegated to trusted subordinates, but the responsibility will ultimately be always of the designated owner.

6.4 Business Impact Assessment

A Business Impact Assessment (BIA) is conducted on all FNWI's systems in order to determine their criticality. A system is defined as critical if at least one of the CIA indicators has a HIGH score. The BIA is carried out by interviewing the system owners and by filling the table provided in *Appendix II: Business Impact Assessment forms*.

6.5 Risk assessment and implementation

Following the BIA, a Risk Assessment is conducted for each system identified as critical. The Risk Assessment procedure should be carried out by the owner of the given information system and assisted by a security supervisor. In this process, opinions, know-how and experiences from all the business representatives interacting with the system should be gathered together in order to include all known points of contact with the system. This process should identify all possible threats and vulnerabilities in the current use, regardless of the presence already of a security policy (new or previously undetected risks might still arise!). The identified threats are then coupled with the possibility that they can be exploited or turned into an incident and the impact that it might cause. Based on the identified risk, it should be decided if the risk is acceptable (usually, for low impact or low possibility for an incident to occur), if there is the need to implement countermeasures to mitigate the risk, or if the risk could be completely avoided (by deciding to totally avoid that piece of system or process, because the risk is not worth it). Specific guidelines should be taken based on ISO 27005.

The countermeasures defined to mitigate risks should be well defined, with clear steps and procedures to apply and assigned responsibilities.

Once the control are in place to mitigate the risk on a specific system, the risk assessment should be performed again, to verify that no new threats have arisen by the implementation of the controls and also to decide if the remaining risk should be controlled further or if it is now acceptable.

6.6 Information security review

Information security expects then to be regularly reviewed. An auditor should review if all the controls specified in the policy are actually implemented and if the policy is enforced.

Also the Risk Assessment process should be performed periodically: in an educational and technologically environment such as the FNWI this should be done ideally each year. The reason is that many things may change with time: new laws and regulation might influence directly or indirectly how information security should be handled (e.g. change in specific processes). Additionally, advancements in technology, new discovered vulnerabilities, addition, modification or deprecation of systems will have an impact on the whole information system infrastructure, which then needs to be re-assessed.

Finally, as described in *Management approval*, the security policy is periodically reviewed by the CISO. It is subjected to the final review by the Faculty Board and needs to be explicitly approved by the Faculty Assembly.

7 Organisation of information security

7.1 End-responsibility

The whole process of preparing and maintaining an Information Security policy is based on a chain of trust and responsibilities, in order to better manage an otherwise huge task for a single person. Still, in the end, the final responsibility is of the Faculty Dean, even if he delegated and appointed responsibility down the hierarchy.

7.2 Faculty Board

The Faculty Board could be involved during the Risk Assessment process, depending if there are processes exclusively related to the Board's scope.

The Faculty Board is also responsible to select an appropriate external Auditor for the review of the actual application of the policy throughout the FNWI.

Ultimately, as described in *Management approval*, the Faculty Board is responsible for the final review of the policy, together with the CISO, before it is submitted to the Faculty Assembly.

7.3 Faculty Assembly

As described in *Management approval*, the Faculty Assembly approves the reviewed Information Security policy.

7.4 Head of Department

With the help of an officer of the ICT department, the Head of each department will draw up the inventory of the information systems involved in their specific department.

Once the inventory is complete, the considered piece of information system is assigned an owner, which usually is the Head of Department in which it is used. A Head of Department owner of a system, is also responsible, in time, to inform the ICT about any update in the inventory of said system.

During the BIA process, the Head of Department is interviewed by the CISO in order to properly assess the potential consequences, should an incident occur.

If a system is identified as having a critical risk, the Head of Department of that system, together with the CISO, identifies possible threats or vulnerabilities and defines the best way of action. He is then responsible to implement and enforce the proper controls deriving from

Baselines or from the Risk Assessment controls to mitigate the possibility of an incident to occur.

Of course, all the tasks that are expected to be performed by the Head of Department can be delegated to a trusted subordinate, but this possibility does not apply to ownership or responsibility of a system.

7.5 ICT department

The ICT department is in charge of setting up and maintaining the FNWI's infrastructure. They are responsible for implementing the controls concerning the FNWI's network and the assets under their control. These controls can derive both from the Baselines and from the outcome of the Risk Assessment.

The ICT department is also involved in the inventory of all the systems, together with the Head of each department. The department is responsible for managing and protecting the inventory list as well as making the relevant changes when notified by the owner of a system.

Given its large influence in the FNWI's business, the ICT is committed to provide aid and advice when a Risk Assessment is conducted in order to ensure a more accurate evaluation.

7.6 Auditor

The auditor is an external certified entity which is appointed to conduct the audit on the FNWI's information systems. The audit is required to analyse the actual enforcement of the controls deriving from the Baselines and the Risk Assessment as well as the evaluation of the current security policy. The audit needs to assess the security of FNWI in all its aspects.

7.7 Chief Information Security Officer

The Chief Information Security Officer (CISO) is appointed to periodically review the information security policy of FNWI. He is also in charge of notifying the Faculty Board when information security is not enforced.

The CISO is responsible for carrying out the Business Impact Assessment through the usage of the forms provided in *Appendix II: Business Impact Assessment forms*. The forms are filled only after a discussion with the owner of the system.

The CISO is committed to evaluate the security of the systems and the enforcement of the security policy.

The CISO is appointed to periodically conduct the Risk Assessment on the FNWI's information systems.

7.8 Employees and students

Employees and students are expected to be aware of the FNWI's security policy and to act accordingly during their daily use of the faculty's services, systems or processes.

They could be involved during the Risk Assessment for a specific system in which they are involved as a sample population of all user interacting with said system. This is done to allow a better understanding of possible points of failure across all possible users.

Appendix I: Baselines

ISO 27002 #	Title	Selected Y/N	Motivate why not selected or in keywords which parts.
A5	Information security policies		
A5.1	Management direction for information security		
A5.1.1	Policies for information security	Y	
A5.1.2	Review of the policies for information security	Y	
A6	Organisation of information security		
A6.1	Internal organisation		
A6.1.1	Information security roles and responsibilities	Y	
A6.1.2	Segregation of duties	Y	
A6.1.3	Contact with authorities	N	Not relevant to every system
A6.1.4	Contact with special interest groups	Y	a) Improve knowledge, c) early warnings
A6.1.5	Information security in project management	N	Not relevant to every system
A6.2	Mobile devices and teleworking		
A6.2.1	Mobile device policy	N	Not relevant to every system
A6.2.2	Teleworking	N	Not relevant to every system
A7	Human resource security		
A7.1	Prior to employment		
A7.1.1	Screening	Y	
A7.1.2	Terms and conditions of employment	Y	
A7.2	During employment		
A7.2.1	Management responsibilities	Y	
A7.2.2	Information security awareness, education and training	Y	
A7.2.3	Disciplinary process	Y	
A7.3	Termination and change of employment		
A7.3.1	Termination or change of employment responsibilities	Y	
A8	Asset management		
A8.1	Responsibility for assets		
A8.1.1	Inventory of assets	Y	
A8.1.2	Ownership of assets	Y	
A8.1.3	Acceptable use of assets	Y	
A8.1.4	Return of assets	Y	
A8.2	Information classification		
A8.2.1	Classification of information	N	Not relevant to every system
A8.2.2	Labelling of information	N	Classification scheme not implemented
A8.2.3	Handling of assets	N	Classification scheme not implemented
A8.3	Media handling		
A8.3.1	Management of removable media	Y	
A8.3.2	Disposal of media	Y	
A8.3.3	Physical media transfer	N	Not relevant to every system
A9	Access control		
A9.1	Business requirements of access control		

A9.1.1	Access control policy	Y	
A9.1.2	Access to networks and network services	Y	
A9.2	User access management		
A9.2.1	User registration and de-registration	Y	
A9.2.2	User access provisioning	Y	e) adapting or removing access rights of users
A9.2.3	Management of privileged access rights	N	Not relevant to every system
A9.2.4	Management of secret authentication information of users	Y	
A9.2.5	Review of user access rights	N	Not relevant to every system
A9.2.6	Removal or adjustment of access rights	Y	
A9.3	User responsibilities		
A9.3.1	Use of secret authentication information	Y	
A9.4	System and application access control		
A9.4.1	Information access restriction	Y	
A9.4.2	Secure log-on procedures	Y	
A9.4.3	Password management system	Y	
A9.4.4	Use of privileged utility programs	N	Not relevant to every system
A9.4.5	Access control to program source code	N	Not relevant to every system
A10	Cryptography		
A10.1	Cryptographic controls		
A10.1.1	Policy on the use of cryptographic controls	N	Not relevant to every system
A10.1.2	Key management	N	Not relevant to every system
A11	Physical and environmental security		
A11.1	Secure areas		
A11.1.1	Physical security perimeter	Y	
A11.1.2	Physical entry controls	N	Not relevant to every system
A11.1.3	Securing offices, rooms and facilities	N	Not relevant to every system
A11.1.4	Protecting against external and environmental threats	Y	
A11.1.5	Working in secure areas	N	Not relevant to every system
A11.1.6	Delivery and loading areas	N	Not relevant to every system
A11.2	Equipment		
A11.2.1	Equipment siting and protection	Y	
A11.2.2	Supporting utilities	N	Not relevant to every system
A11.2.3	Cabling security	Y	
A11.2.4	Equipment maintenance	Y	
A11.2.5	Removal of assets	N	Not relevant to every system
A11.2.6	Security of equipment and assets off-premises	N	Not relevant to every system
A11.2.7	Secure disposal or reuse of equipment	Y	
A11.2.8	Unattended user equipment	N	Not relevant to every system
A11.2.9	Clear desk and clear screen policy	N	Not relevant to every system
A12	Operations security		
A12.1	Operational procedures and responsibilities		
A12.1.1	Documented operating procedures	N	Not relevant to every system
A12.1.2	Change management	Y	
A12.1.3	Capacity management	Y	
A12.1.4	Separation of development, testing and operational environments	N	Not relevant to every system

A12.2	Protection from malware		
A12.2.1	Controls against malware	Y	
A12.3	Backup		
A12.3.1	Information backup	N	Not relevant to every system
A12.4	Logging and monitoring		
A12.4.1	Event logging	Y	
A12.4.2	Protection of log information	Y	
A12.4.3	Administrator and operator logs	N	Not relevant to every system
A12.4.4	Clock synchronisation	Y	
A12.5	Control of operational software		
A12.5.1	Installation of software on operational systems	Y	
A12.6	Technical vulnerability management		
A12.6.1	Management of technical vulnerabilities	N	Not relevant to every system
A12.6.2	Restrictions on software installation	N	Not relevant to every system
A12.7	Information systems audit considerations		
A12.7.1	Information systems audit controls	N	Not relevant to every system
A13	Communications security		
A13.1	Network security management		
A13.1.1	Network controls	Y	
A13.1.2	Security of network services	Y	
A13.1.3	Segregation in networks	Y	
A13.2	Information transfer		
A13.2.1	Information transfer policies and procedures	N	Not relevant to every system
A13.2.2	Agreements on information transfer	N	Not relevant to every system
A13.2.3	Electronic messaging	N	Not relevant to every system
A13.2.4	Confidentiality or nondisclosure agreements	N	Not relevant to every system
A14	System acquisition, development & maintenance		
A14.1	Security requirements of information systems		
A14.1.1	Information security requirements analysis and specification	N	Not relevant to every system
A14.1.2	Securing application services on public networks	N	Not relevant to every system
A14.1.3	Protecting application services transactions	N	Not relevant to every system
A14.2	Security in development and support processes		
A14.2.1	Secure development policy	N	Not relevant to every system
A14.2.2	System change control procedures	N	Not relevant to every system
A14.2.3	Technical review of applications after operating platform changes	Y	
A14.2.4	Restrictions on changes to software packages	N	Not relevant to every system
A14.2.5	Secure system engineering principles	Y	
A14.2.6	Secure Development Environment	N	Not relevant to every system
A14.2.7	Outsourced development	N	Not relevant to every system
A14.2.8	System security testing	N	Not relevant to every system
A14.2.9	System acceptance testing	Y	
A14.3	Test data		
A14.3.1	Protection of test data	N	Not relevant to every system

A15	Supplier relationships		
A15.1	Information security in supplier relationships		
A15.1.1	Information security policy for supplier relationships	Y	
A15.1.2	Addressing security within supplier agreements	Y	
A15.1.3	ICT supply chain	N	Not relevant to every system
A15.2	Supplier service delivery management		
A15.2.1	Monitoring and review of supplier services	N	Not relevant to every system
A15.2.2	Managing changes to supplier services	N	Not relevant to every system
A16	Information security incident management		
A16.1	Management of information security incidents & improvements		
A16.1.1	Responsibilities and procedures	Y	
A16.1.2	Reporting information security events	Y	
A16.1.3	Reporting information security weaknesses	Y	
A16.1.4	Assessment of and decision on information security events	Y	
A16.1.5	Response to information security incidents	Y	
A16.1.6	Learning from information security incidents	Y	
A16.1.7	Collection of evidence	Y	
A17	Information security aspects of Business Continuity Management		
A17.1	Information security continuity		
A17.1.1	Planning information security continuity	N	Not relevant to every system
A17.1.2	Implementing information security continuity	N	Not relevant to every system
A17.1.3	Verify, review and evaluate information security continuity	N	Not relevant to every system
A17.2	Redundancies		
A17.2.1	Availability of information processing facilities	Y	
A18	Compliance		
A18.1	Compliance with legal and contractual requirements		
A18.1.1	Identification of applicable legislation and contractual requirements	Y	
A18.1.2	Intellectual property rights	Y	
A18.1.3	Protection of records	N	Not relevant to every system
A18.1.4	Privacy and protection of personally identifiable information	Y	
A18.1.5	Regulation of cryptographic controls	N	Not relevant to every system
A18.2	Information security reviews		
A18.2.1	Independent review of information security	Y	
A18.2.2	Compliance with security policies and standards	Y	
A18.2.3	Technical compliance review	Y	

A blank cell in the keyword column for Y identifies a full implementation of the control.

Appendix II: Business Impact Assessment forms

Classification of Confidentiality

Business consequences of unintended or unauthorised disclosure of information(worst case)					
Ref	**Question**	**Impact** (circle the answer)			**Motivation**
C01	What will be the reputation loss in case of a compromising of confidentiality ?	Low (Not a real issue)	Medium (Quite some loss, it affects the process)	High (The process might be interrupted)	
C02	What percentage of data is confidential?	0-30 %	30-60%	60-100%	
C03	How much time is required to recover from an information leakage?	< 1 day	1-2 days	> 2 days	
C04	Does the leak expose employees, student or guests to financial loss?	No	Yes but indirectly	Yes, directly	
C05	What will be the legal consequences in case of a leak?	Low (<10000€)	Medium (10000-100000€)	High (>100000€)	
Result (check one of the three boxes)		LOW	MEDIUM	HIGH	

Classification of Integrity

Business Consequences of errors in information or of deliberate manipulation of information to perpetrate or conceal fraud (worst case)					
Ref	**Question**	**Impact** (circle the answer)			**Motivation**
Q01	To what extent the corruption of data affects the process	Low (Not a real issue)	Medium (it affects the process)	High (The process might be interrupted)	
Q02	What is the percentage of information for which integrity is essential?	0-30 %	30-60%	60-100%	
Q03	What would be the financial loss in case of corruption of data?	< 10000€	10000-100000€	>100000€	
Q04	What percentage of data is recoverable in case of compromising?	60-100%	60-30%	30-0 %	
Q05	Possible follow up incident due to corrupted data?	None	Some	A lot	
Result (check one of the three boxes)		LOW	MEDIUM	HIGH	

Classification of Availability

Business Consequences of a prolonged outage of the system(worst case)					
Ref	**Question**	**Impact** (circle the answer)			**Motivation**
A01	What is the percentage of activities that cannot work in case of unavailability of systems?	0-30 %	30-60%	60-100%	
A02	How much working time is needed to restore the service?	< 4h	4-12h	> 12h	
A03	How long can the system be unavailable before a significant financial loss (50k) occurs?	> 1 week	1-7 days	< 1 day	
A04	How long can the system be unavailable before reputation is affected?	<1 day	1-7 days	> 1 week	
A05	Can a temporary solution be set up?	Yes	Yes, for 1-3 days	No	
Result (check one of the three boxes)		LOW	MEDIUM	HIGH	