Security in Organizations: Assignment 3

Group number 27

Elwin Tamminga
s1013846

Lucas van der Laan
s1047485

1 Introduction

The Faculty of Science is a department of the University of Radboud Nijmegen that is responsible for the study on the sciences at Radboud. The sciences include the fields of Molecular Sciences, Biosciences, Computing- and Information Sciences, and Mathematics and Physics & Astronomy. The faculty handles not only the education of the students, but also does research into the fields that it teaches the students about. This document provides the information security policy to ensure the information security for the business processes of the faculty.

The types of business processes of the faculty are:

- Education – The faculty is focused on teaching the students, so education is part of the main business processes.
- Research – A lot of the professors at the faculty also perform research into their expertise and publish papers on that.
- Developing technologies, like the High Field Magnet Laboratory, which is then used for research.
- Designing a curriculum for students that study at the faculty.
- Helping students with their research when needed.
- Managing (corporate or strategic, decisions)
- Supporting (accounting, human resource management, technical support).

All the departments can be see in Appendix A, using the oraganogram. The core departments are the departments that make the faculty money and/or that help the faculty in reaching it's goal. This means that the core departments are:

- Education Institutes
- Research Institutes
- Faculty Board

The supporting departments are the service departments, as they help the core departments with their goal and to keep them running.

The following external parties provides systems used by the whole university, so the faculty also depends on it. These systems are not managed by the faculty but are under control of the department of Academic Affairs of the university:

- CACI provides OSIRIS which is used for enrollments and grading.
- D2L provides Brightspace which is used for providing course content, assignments and livestreams.
- SURF provides the network structure and services to allow users of the university to log in and connect to different IT systems.
- Microsoft provides the account and mail system for the univesity.
- KUARIO provides the printing system on the university.

2 Definition of information security

Information security is defined as the preservation of confidentiality, integrity, and availability of information (*ISO/IEC 27000:2014* 2014).

- Confidentiality – Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- Integrity – Property of accuracy and completeness.
- Availability – Property of being accessible and usable upon demand by an authorized entity.

This is relevant for the following core processes:

- Education – Availability is the most important property for systems like Brightspace, where students can access course material. Integrity is the most important property for OSIRIS, because results should not be changed by students.
- Research – Depending on the research, different aspects of information security may be more important. If the research is very confidential, then confidentiality is the most important property. If the research is not so confidential but the researchers need high availability of the systems they use, then the availability of those systems are very important. Integrity is also important so the data used during the research can be trusted. So it changes based on the research what aspect is more important.

- Faculty Board management – The faculty makes decisions about how the faculty should be run, this means that integrity and availability of the systems they use to make a decision are very important, so everyone can at any time see correct information about decisions that the faculty board has made. The faculty board also has a need for integrity, so they know that the information that they get is accurate and not distorted.

3 Management approval

The management of the Faculty of Science is structured below:

- Dean
- Vice Deans + Administrative Director
- Branches:
    - Education
        - Scientific Director
    - Special Units
        - Managing Director (only ISE)
        - Director
        - Coordinator
    - Research
        - Managing Director
        - Scientific Director
    - Service Department
        - Department Head

This information security policy is written by the security officer and approved by the Faculty Board of the Faculty of Science. The policy will also be reviewed annually by the security officer and approved by the Faculty Board. The security officer must discuss the policy with all relevant members of the Faculty of Science during the review. Requests for changes are taken into account by the security officer for the next version of the policy.

4 Security objectives

The Faculty of Science requires that the CIA triangle is as secure as possible as it handles not only research, which may be confidential, but it also handles student information. Student information is required to be very secure since the General Data Protection Regulation (GDPR), so if any information related to the GDPR leaks the Faculty can get into a lot of trouble. Important data used in the core processes of the faculty should also be available and the integrity should be kept, because without integrity the Faculty can not verify whether or not the students legitimately passed their courses and they also have to preserve integrity so the students can study well and so the researchers have all their data validated.

Possible threats for the Faculty of Science include:

- Someone hacking the grading system, this leads to falsified grades which can lead to a falsified diploma.
- Database leak, which can leak student information.
- Research data compromised.
- Denial-of-Service attack.
- Ransomware, which could not only cause a Denial of Service, but also important data being lost.

Part of the security objectives are the regulations, legislation and contracts that the Faculty of Science needs to adhere to. These include the Dutch implementation of the General Data Protection Regulation (GDPR), which is the Algemene verordening gegevensbescherming (AVG) and the Dutch Telecommunications Act (TA). The Faculty of Science also needs to implement security controls enforced by contracts with external parties.

These security objective also applies to systems of third parties mentioned in chapter 1. For example, the integrity of the grading system depends on OSIRIS. And to prevent a Denial-of-Service attack or database leak multiple third parties are involved, including D2L (Brightspace), SURF and Microsoft.

5 Scope

The scope of this policy are all systems inside the buildings of the Faculty of Science, like the Huygens building and Mercator 1, and all other systems, communications and stored data used by the Faculty of Science maintained by the faculty or a third party. All members and relevant third parties who uses or are connected to the systems of the Faculty of Science must comply with this policy. Included in the scope but not limited to:

- Science Email server
- Science VPN server
- OSIRIS
- Brightspace
- Physical access to servers
- Printing system

6 Approach

The security officer is responsible for maintaining, reviewing and updating the baselines based on the ISO 27002 (Appendix I) using a combined approach. The combined approach results in a limited baseline security with more focus on the most important business processes and sensitive systems. This prevents unnecessary security controls and makes it easier to see which security controls will have the most effect.

All the information systems should be regularly inventoried by going through all the systems that the faculty maintains itself and all the systems that the faculty pays for. This inventorization should include checking whether or not the systems are still needed and should include a security analysis on every system that is included. All the system should be secure and up-to-date, unless they are specifically designed not to be, due to any valid reason, like for educational assignments. If this is the case, the system should not have any connection to any important systems, which could cause a vulnerability.

Every system that the faculty maintains should have someone that is responsible for or owns said system. If it is unclear who owns the system, this should be settled by selecting someone that should be responsible for the system. The ownership of the system is allocated to the closest business process. The owner of that business process is then also responsible for the system until someone suitable has been found.

High level risk assessments are conducted using a Business Impact Analysis (BIA). This analysis is performed using Business Impact Assessment forms (Appendix II) by the security officer with the help of the business process owners. This will identify the systems with the highest risks for each classification of the CIA triangle (Confidentiality, Integrity and Availability). On these systems risk assessments will be conducted based on the ISO 27005 standard, which outlines the recommended approach for the risk assessment.

The baseline and controls from the risk assessments will be implemented by the security officer with the help of the business process owners. The security officer should ensure that the security controls are actually implemented.

Information security will be secured by ensuring that all the controls of the ISO 27002 are implemented properly, this has to be done at least annually like outlined in section 3 (Management approval). The management review by the Faculty Board will look at all the requirements of ISO 27001 9.3. These requirements are the minimum that have to be completed, so it is not limited to these requirements.

7 Organization of information security

To ensure the Plan-Do-Check-Act (PDCA) cycle using the processes above, the members of the Faculty of Science are divided into the following roles and responsibilities.

7.1 End-responsibility

The dean is responsible for assigning ownership of security sensitive systems to the owner of the corresponding business process. The dean should also ensure that the security officer role is fulfilled and assigned to the correct person.

7.2 (Line) management

Management has to do the management review of the information security. Management is responsible for information security review approval.

7.3 Support departments

Support departments are responsible for assisting the security officer with discussing and implementing security controls.

7.4 ICT department

The ICT department is responsible for the inventory of the systems, they have to know exactly which systems are in use by the faculty, internal and external. If they do not know what a system is for, they should contact the owner and verify that it is still required.

7.5 Internal audit department

The internal audit department is an independent department that makes sure that the risk assessment is properly implemented.

7.6 Corporate security officer

The security officer is responsible for implementing and managing the (baseline) security controls. The security officer is also responsible for conducting (high level) risk assessments and updating the information security policy.

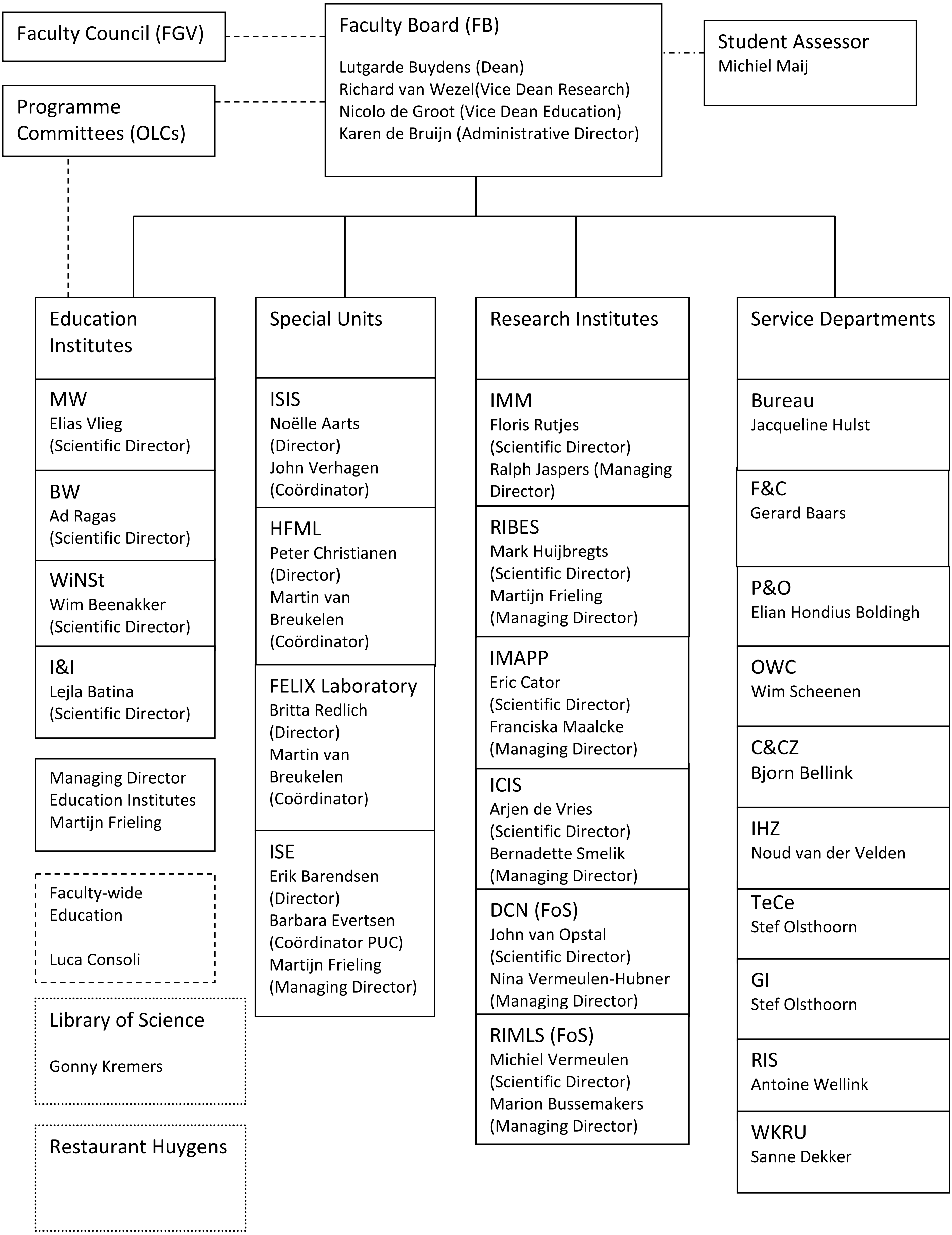
7.7 Employees

Employees have the responsibility to ensure that all the correct controls and protocols are followed that are outlined by the information security policy. Employees have the responsibility to assist the security officer whenever required and requesting changes when needed.

A Organisation Chart

The organisation chart was found on the website of the faculty (*Organogram Faculty of Science 2021* 2021). The organogram is on the next two pages, page 1 has the diagram and page 2 has clarifications for all the acronyms.

Faculty of Science
2021



Faculty Council (FGV)

Programme Committees (OLCs)

Faculty Board (FB)

Lutgarde Buydens (Dean)
Richard van Wezel(Vice Dean Research)
Nicolo de Groot (Vice Dean Education)
Karen de Bruijn (Administrative Director)

Student Assessor
Michiel Maij

Education Institutes

MW
Elias Vlieg
(Scientific Director)

BW
Ad Ragas
(Scientific Director)

WiNSt
Wim Beenakker
(Scientific Director)

I&I
Lejla Batina
(Scientific Director)

Managing Director Education Institutes
Martijn Frieling

Faculty-wide Education

Luca Consoli

Library of Science

Gonny Kremers

Restaurant Huygens

Special Units

ISIS
Noëlle Aarts
(Director)
John Verhagen
(Coördinator)

HFML
Peter Christianen
(Director)
Martin van Breukelen
(Coördinator)

FELIX Laboratory
Britta Redlich
(Director)
Martin van Breukelen
(Coördinator)

ISE
Erik Barendsen
(Director)
Barbara Evertsen
(Coördinator PUC)
Martijn Frieling
(Managing Director)

Research Institutes

IMM
Floris Rutjes
(Scientific Director)
Ralph Jaspers (Managing Director)

RIBES
Mark Huijbregts
(Scientific Director)
Martijn Frieling
(Managing Director)

IMAPP
Eric Cator
(Scientific Director)
Franciska Maalcke
(Managing Director)

ICIS
Arjen de Vries
(Scientific Director)
Bernadette Smelik
(Managing Director)

DCN (FoS)
John van Opstal
(Scientific Director)
Nina Vermeulen-Hubner
(Managing Director)

RIMLS (FoS)
Michiel Vermeulen
(Scientific Director)
Marion Bussemakers
(Managing Director)

Service Departments

Bureau
Jacqueline Hulst

F&C
Gerard Baars

P&O
Elian Hondius Boldingh

OWC
Wim Scheenen

C&CZ
Bjorn Bellink

IHZ
Noud van der Velden

TeCe
Stef Olsthoorn

GI
Stef Olsthoorn

RIS
Antoine Wellink

WKRU
Sanne Dekker

Faculty Council (FGV)
Representative Council (OC)
Faculty Student Council (FSR)

Programme Committees (OLCs)
Biosciences
Computing Science and Information Sciences
Molecular Life Sciences
Physics & Astronomy
Science
Chemistry
Mathematics

Research Institutes
Institute for Molecules and Materials (IMM)
Radboud Institute for Biological and Environmental Sciences (RIBES)
Institute for Mathematics, Astrophysics and Particle Physics (IMAPP)
Institute for Computing and Information Sciences (ICIS)
Donders Centre for Neuroscience (DCN FoS)
Radboud Institute for Molecular Life Sciences (RIMLS FoS)

Special Units
Institute for Science in Society (ISIS)
High Field Magnet Laboratory (HFML)
FELIX Laboratory (FELIX)
Institute for Science Education (ISE)

Education Institutes
Molecular Sciences (MW)
- Molecular Life Sciences (BSc and MSc)
- Science (BSc and MSc)
- Chemistry (BSc and MSc)

Biosciences (BW)
- Biology (BSc and MSc)
- Medical Biology (MSc)

Computing Science and Information Sciences (I&I)
- Computing Science (BSc and MSc)
- Information Sciences (MSc)

Mathematics and Physics & Astrnomy (WiNSt)
- Physics & Astrnomy (BSc and MSc)
- Mathematics (BSc and MSc)

Service Departments
Faculty Office (Bureau)
Finance and Control (F&C)
HR Department (P&O)
Education Centre (OWC)
Computers and Communication (C&CZ)
Building Facility Services (IHZ)
TechnoCentre (TeCe)
General Instruments (GI)
Radboud Innovation Science (RIS)
Science Education Hub Radboud University (WKRU)

November 2021

B Appendix I & II

Security in Organizations: Assignment #3

Appendix I Baselines

Statement of Applicability and status of information security controls			
#	**Title**	**Selected Y/N**	**Motivation**
A5	Information security policies		
A5.1	Management direction for information security		
A5.1.1	Policies for information security	Y	Required by legislation
A5.1.2	Review of the policies for information security	Y	To ensure that the security stays intact
A6	Organization of information security		
A6.1	Internal organization		
A6.1.1	Information security roles and responsibilities	Y	If this is not done, the faculty is vulnerable.
A6.1.2	Segregation of duties	Y	The faculty should only allow employees to do as they require, especially since some employees are in service of multiple employers.
A6.1.3	Contact with authorities	Y	A university body should always have contact with legislative bodies to ensure that they are following the rules.
A6.1.4	Contact with special interest groups	N	Not required as it’s a university

			with experts in the field.
A6.1.5	Information security in project management	Y	Information Security is a core process, so it should be included.
A6.2	Mobile devices and teleworking		
A6.2.1	Mobile device policy	N	Nothing important should ever be stored on a mobile device.
A6.2.2	Teleworking	Y	The faculty has a VPN that needs to be secured.
A7	Human resource security		
A7.1	Prior to employment		
A7.1.1	Screening	Y	Any employee that deals with private or secret information should be screened so nothing leaks.
A7.1.2	Terms and conditions of employment	Y	Employees should not be allowed to leak information and notify higher ups about bad practice if they see it.
A7.2	During employment		
A7.2.1	Management responsibilities	Y	Employees should not be allowed to leak information and notify higher ups about bad practice if they see it.

A7.2.2	Information security awareness, education and training	Y	To ensure that best practices are followed.
A7.2.3	Disciplinary process	Y	Information Security is crucial
A7.3	Termination and change of employment		
A7.3.1	Termination or change of employment responsibilities	Y	To ensure that they do not leak information that they learned while they were employed.
A8	Asset management		
A8.1	Responsibility for assets		
A8.1.1	Inventory of assets	Y	To ensure that obsolete assets no longer hold information that can leak.
A8.1.2	Ownership of assets	Y	To ensure that all the assets have someone responsible.
A8.1.3	Acceptable use of assets	Y	The faculty has systems that can do harm, thus they should only be used for their respectable uses.
A8.1.4	Return of assets	N	The faculty should be capable of terminating anything remotely.
A8.2	Information classification		
A8.2.1	Classification of information	N	Not every control can be implemented, this control is not

			important enough.
A8.2.2	Labelling of information	Y	Information related to students should be labeled as such.
A8.2.3	Handling of assets	N	Related to A8.2.1
A8.3	Media handling		
A8.3.1	Management of removable media	Y	Research data is very important to keep secret until publication.
A8.3.2	Disposal of media	Y	Media should not contain any information and should be securely wiped before disposal.
A8.3.3	Physical media transfer	Y	Scientific information should always be protected against danger at all costs.
A9	Access control		
A9.1	Business requirements of access control		
A9.1.1	Access control policy	Y	Only those responsible should have access to student data, for example.
A9.1.2	Access to networks and network services	Y	The Faculty has a VPN
A9.2	User access management		
A9.2.1	User registration and de-registration	Y	If someone leaves the faculty,

			they should no longer have access to secret research.
A9.2.2	User access provisioning	Y	Users should only have access to that which concerns them.
A9.2.3	Management of privileged access rights	N	This should be done by the IT department
A9.2.4	Management of secret authentication information of users	Y	Authentication information for faculty personnel is very important.
A9.2.5	Review of user access rights	Y	To ensure that someone does not have access rights when they no longer are supposed to have them.
A9.2.6	Removal or adjustment of access rights	N	This falls under A9.2.1
A9.3	User responsibilities		
A9.3.1	Use of secret authentication information	Y	The only person that should access your account, is you.
A9.4	System and application access control		
A9.4.1	Information access restriction	N	This is limited to every department, not the faculty as a whole.
A9.4.2	Secure log-on procedures	Y	See A9.3.1
A9.4.3	Password management system	Y	See A9.4.2

A9.4.4	Use of privileged utility programs	Y	See A6.1.2
A9.4.5	Access control to program source code	N	The faculty does not produce source code.
A10	Cryptography		
A10.1	Cryptographic controls		
A10.1.1	Policy on the use of cryptographic controls	N	This is done by the university, not the faculty.
A10.1.2	Key management	N	See A10.1.1
A11	Physical and environmental security		
A11.1	Secure areas		
A11.1.1	Physical security perimeter	Y	The faculty systems that need to be protected.
A11.1.2	Physical entry controls	Y	See A11.1.1
A11.1.3	Securing offices, rooms and facilities	Y	See A11.1.1
A11.1.4	Protecting against external and environmental threats	Y	Important data is stored on the systems that need to be kept intact.
A11.1.5	Working in secure areas	Y	It’s a research institute, information needs to be kept secure.
A11.1.6	Delivery and loading areas	N	Not as important.
A11.2	Equipment		

A11.2.1	Equipment siting and protection	Y	Research information, again.
A11.2.2	Supporting utilities	Y	A system that is doing calculations should not short-circuit because of a power surge.
A11.2.3	Cabling security	Y	Cables carry important data.
A11.2.4	Equipment maintenance	Y	Maintenance if very important for security vulnerabilities.
A11.2.5	Removal of assets	Y	Assets can contain confidential information.
A11.2.6	Security of equipment and assets off-premises	Y	See A11.2.5
A11.2.7	Secure disposal or reuse of equipment	Y	See A8.3.2
A11.2.8	Unattended user equipment	Y	Equipment should not be accessible by unauthorized persons.
A11.2.9	Clear desk and clear screen policy	Y	Confidential information should never be on display.
A12	Operations security		
A12.1	Operational procedures and responsibilities		
A12.1.1	Documented operating procedures	Y	When something goes wrong, people have to know what to do.
A12.1.2	Change management	Y	Changes that affect information

			security need to still produce good information security.
A12.1.3	Capacity management	Y	Only required data should be stored and if more is needed then more shall be given.
A12.1.4	Separation of development, testing and operational environments	N	The faculty does not have anything that they develop and need to test.
A12.2	Protection from malware		
A12.2.1	Controls against malware	Y	Systems should be safe against compromised data.
A12.3	Backup		
A12.3.1	Information backup	Y	If any system gets compromised or infected, the data should be store somewhere else.
A12.3	Logging and monitoring		
A12.4.1	Event logging	N	No logs are needed for the faculty.
A12.4.2	Protection of log information	N	See A12.4.1
A12.4.3	Administrator and operator logs	N	See A12.4.1
A12.4.4	Clock synchronization	N	No need for a synchronized clock
A12.5	Control of operational software		

A12.5.1	Installation of software on operational systems	N	All operating systems are linked to the user, so the user can install any program they wish.
A12.6	Technical vulnerability management		
A12.6.1	Management of technical vulnerabilities	Y	Every organization is existence should protect their systems against technical vulnerabilities.
A12.6.2	Restrictions on software installation	N	See A12.5.1
A12.7	Information systems audit considerations		
A12.7.1	Information systems audit controls	Y	Availability is important, thus audit controls need to minimally disrupt availability.
A13	Communications security		
A13.1	Network security management		
A13.1.1	Network controls	Y	Segregation and other controls must be implemented to prevent unauthorized access.
A13.1.2	Security of network services	Y	See A13.1.1.
A13.1.3	Segregation in networks	Y	See A13.1.1.
A13.2	Information transfer		

A13.2.1	Information transfer policies and procedures	Y	Confidential information should be kept secure.
A13.2.2	Agreements on information transfer	Y	The faculty deals with information that can be sen
A13.2.3	Electronic messaging	N	Not important
A13.2.4	Confidentiality or nondisclosure agreements	Y	See A13.2.1
A14	System acquisition, development & maintenance		
A14.1	Security requirements of information systems		
A14.1.1	Information security requirements analysis and specification	Y	Applicable to new and existing sensitive systems that handles student information or sensitive research data.
A14.1.2	Securing application services on public networks	Y	To ensure the privacy of students and to keep private research private.
A14.1.3	Protecting application services transactions	Y	See A14.1.2
A14.2	Security in development and support processes		
A14.2.1	Secure development policy	N	Software used by the faculty is maintained by other companies and is not developed by the faculty.

A14.2.2	System change control procedures	N	See A14.2.1.
A14.2.3	Technical review of applications after operating platform changes	N	See A14.2.1.
A14.2.4	Restrictions on changes to software packages	N	See A14.2.1.
A14.2.5	Secure system engineering principles	N	This control can be implemented at university level.
A14.2.6	Secure Development Environment	N	A14.2.5.
A14.2.7	Outsourced development	Y	This only applies to systems outsourced by the faculty, because the university might not know the systems in detail.
A14.2.8	System security testing	N	See A14.2.1.
A14.2.9	System acceptance testing	N	See A14.2.1.
A14.3	Test data		
A14.3.1	Protection of test data	Y	Required for A18.1 to ensure the privacy of personal data.
A15	Supplier relationships		
A15.1	Information security in supplier relationships		
A15.1.1	Information security policy for supplier relationships	Y	Organizations outside the Faculty of Science should not have access

			to other private information.
A15.1.2	Addressing security within supplier agreements	Y	See A15.1.1
A15.1.3	ICT supply chain	Y	See A15.1.1
A15.2	Supplier service delivery management		
A15.2.1	Monitoring and review of supplier services	N	Most supplier services (e.g. Brightspace, Osiris) are widespread university services and do not specifically fall under the faculty.
A15.2.2	Managing changes to supplier services	N	See A15.2.1
A16	Information security incident management		
A16.1	Management of information security incidents & improvements		
A16.1.1	Responsibilities and procedures	Y	This ensures that an incident won’t affect more systems than necessary.
A16.1.2	Reporting information security events	Y	See A16.1.1
A16.1.3	Reporting information security weaknesses	Y	See A16.1.1
A16.1.4	Assessment of and decision on information security events	Y	See A16.1.1
A16.1.5	Response to information security incidents	Y	See A16.1.1

A16.1.6	Learning from information security incidents	Y	This ensures that incidents won’t happen again.
A16.1.7	Collection of evidence	Y	This is necessary in case very sensitive information is leaked that could affect students or companies.
A17	Information security aspects of Business Continuity Management		
A17.1	Information security continuity		
A17.1.1	Planning information security continuity	N	No need to change the requirements in adverse situations, this may not be the case at university level.
A17.1.2	Implementing information security continuity	Y	Sensitive unpublished research documents (e.g. biological data or new security leaks) should always be secure.
A17.1.3	Verify, review and evaluate information security continuity	Y	Required for A17.1.2
A17.2	Redundancies		
A17.2.1	Availability of information processing facilities	Y	Availability is important for research within the Faculty of Science.
A18	Compliance		
A18.1	Compliance with legal and contractual requirements		

A18.1.1	Identification of applicable legislation and contractual requirements	Y	To ensure compliance. Only the parts that falls under the Faculty of Science only, the rest can be done at university level.
A18.1.2	Intellectual property rights	N	Is not that important for a university, usually products are free to use for students anyway.
A18.1.3	Protection of records	Y	Same as A17.1.2
A18.1.4	Privacy and protection of personally identifiable information	Y	To ensure the privacy of students (and teachers) and required by law.
A18.1.5	Regulation of cryptographic controls	Y	Required for A18.1.3 and A18.1.4
A18.2	Information security reviews		
A18.2.1	Independent review of information security	N	Can be done at university level.
A18.2.2	Compliance with security policies and standards	Y	Will be reviewed by SO.
A18.2.3	Technical compliance review	Y	Required by legislation.

Appendix II - Business Impact Assessment forms

Classification of Confidentiality

Business consequences of unintended or unauthorized disclosure of information (worst case)					
Ref	**Question**	**Impact** (circle the right answer)			**Motivation**
C01	How privacy-sensitive is the information?	Public	Basic (membership, subscription related, employee related)	High (medical, financial, sexual inclination)	
C02	What would happen if security research leaks?	Nothing	Some bad practices come to light	Huge financial loss for the subject of the research.	
C03	Physical access to information systems?	All public information systems	Systems only students can access, student names	Research data, personal student information	
C04	What is the reputation loss?	Nothing	Negative publicity in Netherlands	Worldwide negative publicity	
C05	What happens if the VPN is compromised?	None, only encrypted data visible	Visible DNS requests, possibly privacy sensitive	All data visible, including very privacy sensitive information and/or research data	
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 right answer)			**Motivation**
I01	What if research (test) data is manipulated?	Nothing, low influence on results	Negative impact on the subject of the research	Negative impact on society	
I02	What happens if the VPN data is manipulated?	Nothing	Some adware gets injected into the VPN connection	Connection gets redirected to malicious websites like faccebook.com	
I03	What happens if the mails from/to the mail server are manipulated?	None, few words might be corrupted	Limited leaks of private information	Huge leaks of private information, financial loss, identity fraud	
I04	Manipulated financial data?	None	Limited financial loss	Huge financial loss	
I05	Manipulated student information?	None	Incorrect address	Students accessing data they are not allowed to access	
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 right answer)			**Motivation**
A01	What happens if the VPN is down?	Students cannot access the VPN's	The faculties' services are no	Important research cannot be done because	

		services for a bit	longer accessible	it requires the VPN	
A02	What happens if the email server is down?	People need to use their non-science mail	Some mails ae missed	Important emails for research are lost and make the connection lose trust.	
A03	What happens if the internal systems are down?	The students cannot get access to some data.	Some research gets halted.	The entire faculty loses access and can do nothing.	
A04	What happens if the gitlab server is down?	The Gitlab server is down for a short time.	The faculty members do not have access to the server for a prolonged period of time.	Students that need their Gitlab a day before the deadline don't have access.	
A05	After what downtime do the printers no longer follow the specifications?	> 2 days	< 2 days	< 5 hours	
Result (check one of the three boxes)		Low	Medium	High	

References

ISO/IEC 27000:2014 (2014).
URL: *https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en*

Organogram Faculty of Science 2021 (2021).
URL: *https://www.ru.nl/publish/pages/785232/organogram_faculty_of_science_-_november_2021.pdf*