

Stellenbosch University

Information Security Regulations

1. Preamble

- 1.1. Information Security is a component of the Risk Management structure and procedures of the University.
- 1.2. Stellenbosch University has an obligation to ensure appropriate security for all Information Technology (IT) systems (data, equipment, and processes) and information that it owns and controls. An Information Security Regulation is mandatory: every member of the university (student and/or staff member) shares the obligation to ensure appropriate security, to varying degrees.
- 1.3. Appropriate levels of security must be determined by risk assessment i.e. assessment of threats to, impacts on and vulnerabilities of IT systems and information, and the likelihood of their occurrence.
- 1.4. The need for Information Security is driven by three factors:
 - 1.4.1. Legal, statutory, regulatory and contractual obligations
 - 1.4.2. Risk assessment
 - 1.4.3. Operational principles, objectives and requirements for information systems that the university has defined or developed.

2. **The Rector's Management Team acknowledges and confirms the importance of Information Security and the imperative to minimise information security risks.**

3. **It is the responsibility of the Senior Director: Information Technology to:**

- 3.1. develop and implement policies, regulations, standards, guidelines and organisation, and delegate responsibilities, necessary to minimise the University's information security risks (supplementary regulations that detail scope, organisation and roles are described in Appendix A);
- 3.2. assume leadership, responsibility, and control of responses to information security incidents, threats and breaches.

4. Definition of Information Security¹.

4.1. Security can be defined as "the state of being free from unacceptable risk". The risks can be considered within the following categories of potential losses:

4.1.1. *Confidentiality* of information. Confidentiality means ensuring that information is accessible only to those authorised to have access

4.1.2. *Integrity* of information and processing. Integrity means safeguarding the accuracy and completeness of information and processing methods.

4.1.3. *System availability*. Availability means ensuring that authorised users have access to information and associated assets when required.

4.1.4. *Assets*. The assets owned and/or controlled by the University and that must be protected include:

4.1.4.1. Computer and peripheral equipment.

4.1.4.2. Communications equipment.

4.1.4.3. Computing and communications premises.

4.1.4.4. Power, water, environmental control, and communications utilities.

4.1.4.5. Supplies and data storage media.

4.1.4.6. System computer programs and documentation.

4.1.4.7. Application computer programs and documentation.

4.1.4.8. Information

4.1.5. *Efficient and Appropriate Use*. Efficient and Appropriate Use ensures that University information system assets are used for the purposes for which they were intended, in a manner (i.e. efficient, and not wasteful, use of resources such as storage, bandwidth and processor time) that does not interfere with the reasonable access rights of others.

4.2. The potential causes of these losses are termed "threats". These threats may be human or non-human, natural, accidental, or deliberate.

5. These are interim regulations and will be replaced by an Information Security Policy.

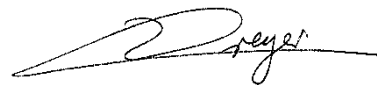
Signed:

RF Pina
Director IT: eBusiness

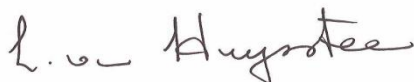


Signed:

MW Dreijer
Senior Director: IT



Signed on behalf of the Rector's Management Team:



Prof L. Van Huyssteen
Executive Director: Operations and Finance
Date: 4 October 2010

¹ We wish to express our gratitude to Murdoch University, Australia, for granting permission for elements of their Information Security Policy to be used in the drafting of this regulation.

APPENDIX A: Information Security scope, roles and organisation

1. Document Hierarchy

1.1. The Information Security Regulations will overlap with existing and emerging policies/regulations (e.g. Electronic Communications Policy, Disaster Recovery Regulation, Privacy Policy, Data Management Regulations, etc. as relevant. Refer to Figure 1: Information Security Policy/Regulation Document Hierarchy). Where this occurs, this regulation will take precedence, provide a cross-referencing framework and refer to the other policies/regulations where appropriate.

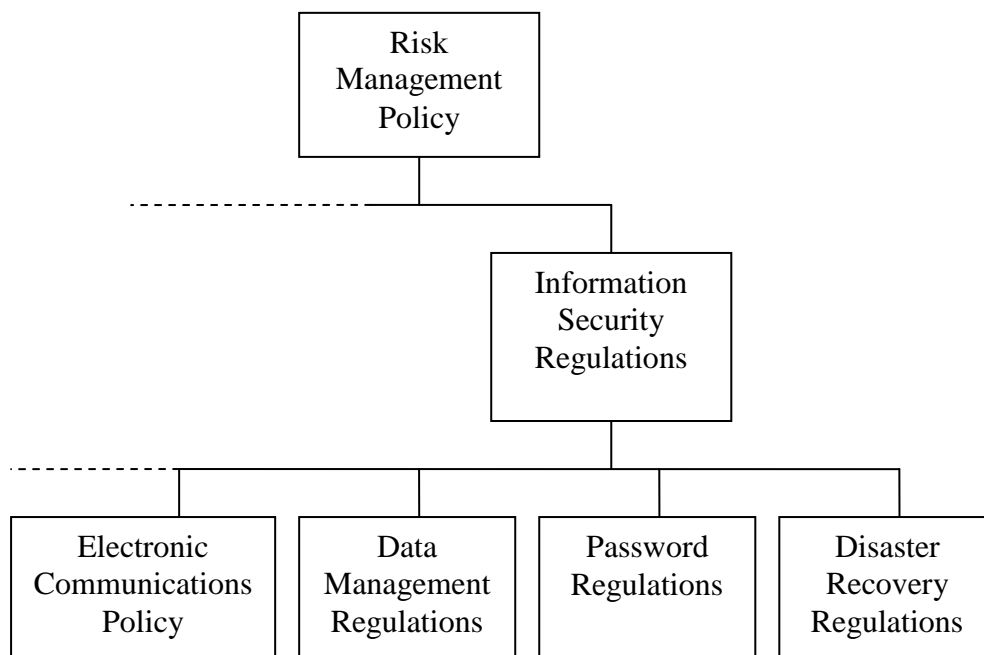


Figure 1: Information Security Policy/Regulation Document Hierarchy

2. The Scope of Information Security.

2.1. Further to the Definition of Information Security as set out above, the following domains and frameworks are described:

2.2. Information Security Domains and Framework.

Policies and regulations that are promulgated in terms of this policy should be structured within the following domains and framework:

2.2.1. **Managerial security**

Roles and organisational structure are defined in a following section.

Administrative security: this includes user training and awareness; reporting of security problems; controls and risk assessment; outsourcing and third party contracts.

Human Resource and Student matters: this includes discipline and consequences; qualifications and skills; backup people; background checks.

Business continuity management: this includes disaster recovery planning; contingency planning; testing of plans; identification and minimisation of risks.

2.2.2. Logical security

Software security: this includes system access control and password management; privilege control and logging.

Software development and change control: this includes handling of viruses and worms; the software development process; the change control process including for workstations; third party involvement.

Data security: this includes intellectual property rights; data privacy; data confidentiality; data criticality and data integrity.

Communications security: this includes establishing network connections; flow control systems including firewalls; encryption; dial-up communications; downloaded data; telephone systems; electronic mail systems; telecommuting arrangements; internet connections and electronic payment systems.

2.2.3. Physical security

Physical access security: this includes building and computer facilities' access control.

Computer location and environment: this includes the premises; emergency data centre premises; their construction; power supplies; emergency equipment; alarm systems; contingency plans; etc.

3. Roles and organisational structure

3.1. Regulation Management.

The following organisational structure (refer to Figure 2: Organogram for Information Security), in addition to existing line management structures, is defined in order to govern, manage and implement Information Security on a cross-cutting, institutional basis:

- An Information Security Management Committee, under the chairmanship of the Senior Director: Information Technology as Chief Information Officer (CIO), that functions as a sub-committee of the Risk Management Committee.
- An Information Security Incident Response Team
- An Information Security Officer.

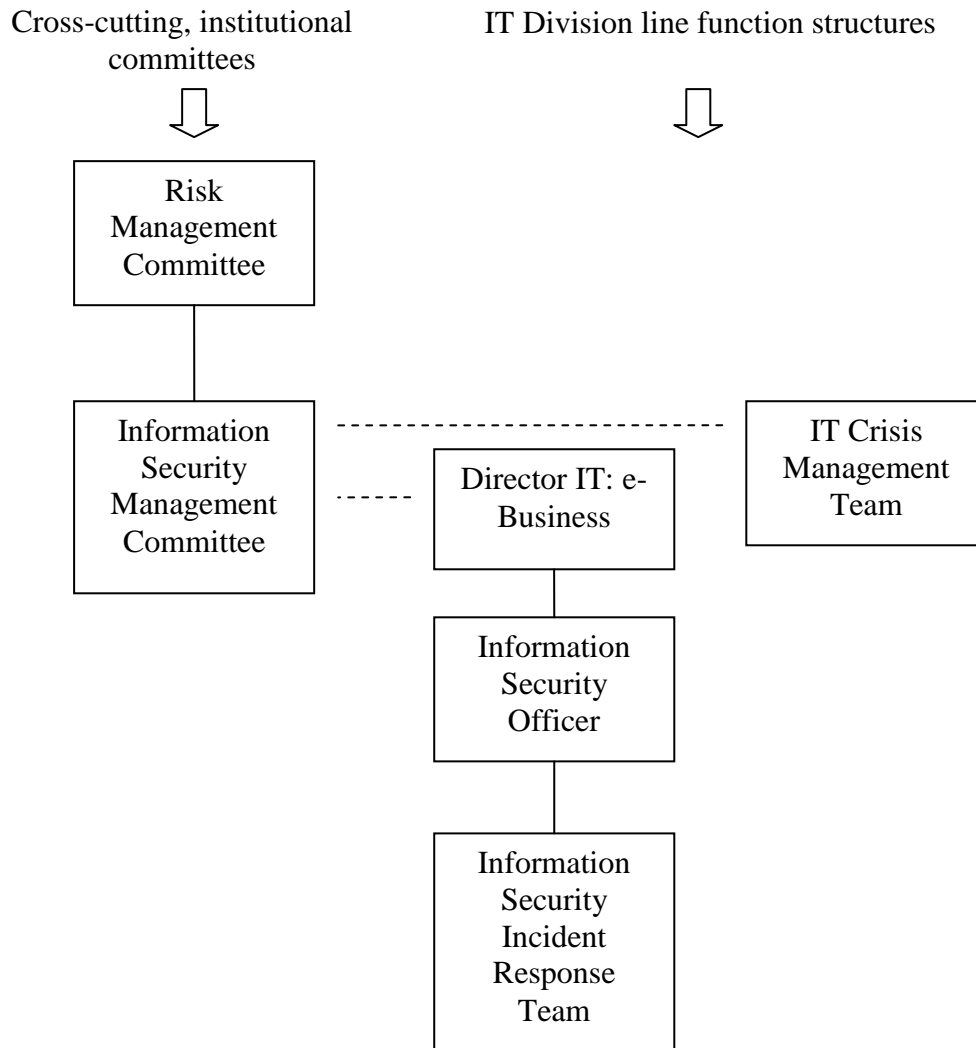


Figure 2: Organogram for Information Security

3.1.1. Information Security Management Committee

The functions of this multi-disciplinary, institutional committee are to:

- Review and approve the Information Security Regulations, subsidiary policies and regulations developed in terms of the Information Security Regulations, and annual Information Security Plan
- Define Information Security responsibilities and appoint responsible persons in Information Security roles across the institution
- Review and monitor major security incidents
- Monitor significant changes in the exposure of IT assets to major threats.
- Initiate and review regular risk assessments
- Report to the Risk Management Committee on Information Security issues
- Advise Executive Management on Information Security issues.

The Information Security Management Committee will comprise², at least:

- The Senior Director IT (Chair)
- A representative from the Internal Audit Committee
- The Chief Director: Finance or a delegate
- The Head: Protection Services or a delegate
- The Chief Director: Human Resources or a delegate
- The Senior Director: Institutional Research and Planning or a delegate
- The Head: Legal Services or a delegate
- The Registrar or a delegate
- The Senior Director: Research Development or a delegate
- An academic staff member from the Department of Information Science
- A Student Representatives Council representative
- The Information Security Officer, as representative of the Information Security Incident Response Team
- The Director IT: eBusiness (Co-ordinator).

The Committee must meet at least quarterly.

² Note that the committee is not required to be representative, but rather that its members have the relevant expertise to make a contribution to managing institutional information security

3.1.2. Information Security Incident Response Team³

The Information Security Incident Response Team will ideally provide the following services in the following service categories:

Reactive services: services triggered by an event or report:

- Disseminating alerts and warnings
- Handling incidents
- Handling vulnerabilities
- Handling artifacts⁴.

Proactive services: services to provide assistance and information to help prepare, protect and secure assets in anticipation of threats:

- Announcements
- Security audits and assessment
- Technology watch
- Guidance on configuration and maintenance of security tools, applications, infrastructures and services
- Preparation and drafting of detailed security regulations, guidelines and standards, as part of the Information Security Regulations. Such documents must be submitted to the Director IT: eBusiness for further managerial review and approval where necessary.
- Preparation of an annual Information Security Plan
- Intrusion detection services
- Provide a security-related information repository.

Security quality management services: assistance with:

- Risk analysis
- Business continuity and disaster recovery planning
- Security consulting
- Awareness building
- Education and training
- Product evaluation or certification.

The Information Security Incident Response Team will comprise:

- The Information Security Officer, who will chair meetings and co-ordinate the team
- All System and Database Administrators in the IT Division
- All System and Database Administrators in divisions and faculties who do not report to the IT Division, as required

³ The Incident Response Team should not be confused with the IT Crisis Management Team that has been created in terms of the IT Crisis Management Plan. The latter comprises the IT Senior Director and Directors and will determine when an Information Security incident escalates into an IT crisis.

⁴ Files or objects found on a system that may be involved in probing, attacking, or circumventing security on systems. These can include viruses, Trojan horse programs, exploit scripts, worms, and toolkits.

- Computer User Area (CUA) Managers as required
- The Manager: IT Support Services
- A communications/media specialist, as required
- Co-opted technical specialists, as required.

3.1.3. Information Security Officer

The Information Security Officer is a technical security expert who is responsible for the sustained management of information security regulations, standards, procedures and technical systems. As such, a key performance area (KPA) of the post involves the co-ordination of the Information Security Incident Response Team. Ideally, the position should be a new and separate post but the KPAs must realistically be delegated to an existing position within the IT Division.

3.2. Custodianship and user responsibilities.

Information Security of each information asset will be the responsibility of its custodian.

3.2.1. Custodians⁵

- The IT Division (IT) will be the custodian of all strategic system platforms and infrastructure.
- IT will be custodian of the strategic communications systems.
- Deans will be custodians of computing laboratories/computer user areas under their respective ownership.
- Divisions, departments and units will be custodians of strategic *applications and information* under their management control (e.g. Finance, Human Resources, Centre for Teaching and Learning, Library).
- Deans and heads of divisions, departments, institutes and units will be custodians of all non-strategic systems under their ownership.
- Individuals will be custodians of desktop systems under their control.

3.2.2. Users

- Each user of the University's information resources, including all staff and students will be responsible for meeting standards of behaviour that are published in terms of this regulation.
- All ordinary users of University information resources:

⁵ Custodians protect and care for assets in their custody.

- Will conform to the policies, regulations, guidelines, standards and codes of practice as promulgated in terms of this regulation from time to time.
- Are responsible for the proper care and use of information resources under their direct control.
- Are obliged to report security incidents to the IT Help Desk or the relevant Computer User Area Managers.
- Are expected to attend required computer security and functional training.
- All special types of users of University IT resources such as contractors, consultants, associates, visiting staff, guests, etc. are required to:
 - Conform to the policies, guidelines, standards and codes of practice as promulgated under this regulation from time to time.
 - Are responsible for the proper care and use of information resources under their direct control.
 - Are obliged to report security incidents to the IT Help Desk or the relevant Computer User Area Managers.

The above conditions must be included in standard terms and conditions that are part of the contracts and agreements that govern the relationships between such users and the University.

A regular audit of information assets should be undertaken, the custodians (and their delegated managers) should be identified, and their responsibilities documented.

4. Regulation review and maintenance cycle.

Review of the Information Security Regulations will be driven by the regular risk assessments initiated by the Management Information Security Committee, or when the Committee considers a review necessary as a result of changes in the environment.

The Information Security Incident Response Team will convene on at least a monthly basis, and will propose policy changes to the Management Information Security Committee where necessary. It will, however, continuously review and adapt detailed policies, regulations, standards, plans and guidelines.