



UNIVERSITEIT
STELLENBOSCH
UNIVERSITY

Interim Access Regulation

Type of Document:	Regulation
Purpose:	To formalise access management to Student Information Systems and Financial System
Approved by:	Senior Director: Information Technology
Date of Approval:	2012/10/15
Date of Implementation:	2012/11/01
Date of Next Revision:	As required
Date of Previous Revision(s):	None
Policy Owner¹:	Vice-Rector: Research, Innovation and Postgraduate Studies
Policy Curator²:	Senior Director: Information Technology
Keywords:	Access Management, access management life-cycle, Student Information System, Financial System
Validity:	In case of differences in interpretation the English version of this policy will be regarded as the valid version.

SU Policies are available at www.sun.ac.za/policies

¹ Policy Owner: Head(s) of Responsibility Centre(s) in which the policy functions.

² Policy Curator: Administrative head of the division responsible for the implementation and maintenance of the policy



UNIVERSITEIT•STELLENBOSCH•UNIVERSITY
jou kennisvennoot • your knowledge partner

Interim Access Regulation

Reference Number	
Purpose	Formalise access management to Student Information Systems and Financial System
Date Of Implementation	1 November 2012
Review Date	
Previous Reviews	
Regulation Owner	Information Security Management Committee
Regulation Curator	Senior Director: Information Technology
Date Of Approval	15 October 2012
Approved By	Senior Director: Information Technology

1. Purpose

The purpose of this regulation is to formalise Access management within the Stellenbosch University's ("University"). This regulation establishes the basic principles for entire access management life-cycle, from provisioning to deprovisioning for the Student Information System (SIS) and Financial System until such time as the Identity and Access Management solution is implemented.

2. Scope

The regulation applies to all staff, students and associates who access the SIS or Financial system.

3. Definitions

Refer to the IT policy definitions document for further descriptions of terminology used in this regulation.

4. Regulation

The University recognises the risks associated with unauthorised access to core University systems and the importance of restricting access to the minimum required to ensure productivity and reduce risk. This regulation defines the guidelines that will be applicable to the SIS and financial systems until such time as the Identity and Access management solution is in place.

5. Provisions

5.1. General

- 5.1.1. A user or line manager must only request the minimum level of access for the user to perform their responsibilities in line with their role requirements.
- 5.1.2. Line Managers must consider all access granted, specifically restricting conflicting access when requesting, reviewing and authorising access.
- 5.1.3. A user must not attempt to gain access to systems to which they have not been granted authorisation to execute their role requirements.
- 5.1.4. Access is not transferable. A user is not permitted to transfer their access to another user by means of sharing their user ID, US number and password. Permitted exceptions to this regulation statement are documented in section 5.5.
- 5.1.5. Evidence of access processing (i.e. the entire access life-cycle) must be retained in a central repository at the Finance division.
- 5.1.6. All regulation statements are equally applicable to normal business users, super users (e.g. system administrators) and powerful users (e.g. where a user is granted with known segregation of duties conflicts).

5.2. Access provisioning

- 5.2.1. The minimum level of access required to execute a user's role will be granted based on the following:
 - 5.2.1.1. A completed access request form.
 - 5.2.1.2. Line Manager authorisation for required programs and security activities.
 - 5.2.1.3. Cost centre owner authorisation for relevant cost centre processing.
 - 5.2.1.4. Line Manager's written consent and justification for powerful users requiring conflicting programs (e.g. create and approve a requisition). This is also applicable to access amendments.

5.3. Access amendments

- 5.3.1. The minimum level of access required to execute a user's role must be maintained for the duration of their employment at the University. User access must be amended to reflect changes in responsibilities based on the following:
 - 5.3.1.1. A completed access request form
 - 5.3.1.2. Line Manager authorisation for new programs required and for the deprovisioning of access no longer required.
 - 5.3.1.3. Cost centre owner authorisation for new cost centre access required and for the deprovisioning of access no longer required.

5.4. Access deprovisioning

- 5.4.1. User access must be deprovisioned on the earlier date of the user leaving the University or no longer requiring access to perform their role.

5.5. Shared user access

- 5.5.1. Shared use of a user account is only permitted based on the following:
 - 5.5.1.1. Line Manager written justification and authorisation for shared user account access.
 - 5.5.1.2. Documentation of processing performed on the shared user account.
- 5.5.2. Only 1 user must be accountable for a user account at any given point in time. This must be documented.

- 5.5.3. Upon taking accountability for a shared user account, the user must change the password at the point of handover.

5.6. Access monitoring

- 5.6.1. The Business System Manager must review users leaving the University or users changing roles against active users on a monthly basis and amend access accordingly.
- 5.6.2. Line Managers must review and authorise user access within their business area on at least an annual basis.

6. Governance

6.1. Governance structure

Changes to this regulation will be initiated by the Information Security Management Committee, whose chair, the Senior Director: IT, will then consult with the necessary line structures and forums in order to have regulation changed.

6.2. Ownership

The regulation is owned by the Information Security Management Committee.

6.3. Approval

This regulation can be approved by the Senior Director: Information Technology.

6.4. Implementation

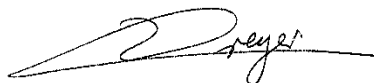
It is the IT department's responsibility to implement the regulation.

6.5. Review

Regulation review will be initiated by the Information Security Management Committee as and when deemed necessary.

6.6. Roles and responsibilities

The Senior Director: IT is the officer responsible for maintaining and implementing the regulation.



Helmi Dreijer
Senior Director: Information Technology