UNIVERSITEIT
STELLENBOSCH
UNIVERSITY

Super User Policy

Type of Document:	Regulation
Purpose:	To protect the integrity of IT resources by controlling super user access.
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 Owner[1]:	Information Security Management Committee
Policy Curator[2]:	Senior Director: Information Technology
Keywords:	Super User, Integrity, Security, IT resources
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

Super User Regulation

Reference Number	
Purpose	To protect integrity of IT resources by controlling super user access
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 protect the integrity of the Stellenbosch University's ("University") IT resources. This regulation aims to limit super user access to authorised and appropriate use.

2. Scope

This regulation applies to all University staff, students and associates, who approve or are granted super user access to University IT resources.

3. Definitions

Refer to the IT policy definitions document for a description of terminology used in this regulation.

4. Regulation

The University requires a limited number of trusted users to be granted with super user access through well-controlled access procedures. In addition, periodic review of super user access is required to validate the on-going need for super user access.

5. Provisions

5.1. General

5.1.1. All super user access requests and amendments must be fully documented detailing the business need and management approval at least at the level of head of division.

5.1.2. The super user's line manager is responsible for ensuring that the user(s) assigned with super user access has all the required knowledge, training, and related skill sets necessary to effectively perform the granted role.

5.1.3. The head of division that submits the request for an individual to be assigned a super user role is ultimately responsible for the work performed under this privileged account. Therefore they are expected to implement internal procedures and/or processes that ascertain that the use of the "Super User" role is appropriate and can be substantiated as required.

5.1.4. The head of division must review and approve all super user access on a bi-annual basis. Documented evidence of this review and the corrective action taken to address any changes required must be retained.

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.

Dreijer

Helmi Dreijer
Senior Director: Information Technology