UNIVERSITEIT STELLENBOSCH UNIVERSITY

Audit Trail Logging and Monitoring

Type of Document:	Regulation
Purpose:	To ensure that audit trails are maintained and reviewed in order to reduce risks.
Approved by:	Information Security Management Committee
Date of Approval:	15 October 2012
Date of Implementation:	1 November 2012
Date of Next Revision:	As needed
Date of Previous Revision(s):	None
Policy Owner[1]:	Information Security Management Committee
Policy Curator[2]:	Senior Director: Information Technology
Keywords:	Audit Trail; Audit Trail Logging; User Accounts; Applications; Systems; Databases; User Activity; Security Violations
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

Audit Trail Logging and Monitoring Regulation

Reference Number	
Purpose	To ensure that audit trails are maintained and reviewed in order to reduce risks.
Date Of Implementation	1 November 2012
Review Date	
Previous Reviews	N/A
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 the Audit trail logging and monitoring of Stellenbosch University's ("University") user accounts. The University requires the means to log and review user activity on the various University applications, systems and databases. In order to accomplish this, and "audit trail" of user activity must be maintained. Audit trails will be used to detect security violations, performance problems and system processing errors.

2. Scope

This regulation applies to all University staff, students and associates, who use, design, implement or administer University systems, programs and databases.

3. Definitions

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

4. Regulation

The University requires a record of users' activity to be maintained and users to be identified and authenticated so that they can be held accountable for their actions. In addition, periodic real-time monitoring of programmer and system– and database administrator transactions are required.

5. Provisions

5.1. General

5.1.1. Audit trails will provide a record or user actions, which will be used to support accountability.

5.1.2. Audit trails will be used to reconstruct events.

5.1.3. Audit trails will be designed and implemented to record appropriate information to assist in intrusion detection.

5.1.4. Audit trails shall be used to identify problems as they occur.

5.2. Audit trail logging

5.2.1. Audit trails must at a minimum specify:

5.2.1.1. Program used to execute the transaction

5.2.1.2. Transaction date and time

5.2.1.3. User ID

5.2.2. The following transactions must be logged:

5.2.2.1. User administrations transactions including user creation, access modifications and access termination

5.2.2.2. System and database administration transactions

5.2.2.3. User login attempts

5.2.2.4. All non-programmatic changes (i.e. via direct access to the database) to database tables, stored procedures, query tables and configurations files

5.2.2.5. Transaction logging should be enabled to facilitate roll-back or recreation in the event of a system or database failure

5.3. Audit trail monitoring

5.3.1. Monitoring mechanisms and/or tools must be deployed to ensure that notifications are sent for critical and abnormal access and change attempts.
Critical: processing, with a high impact on the University
Abnormal: processing, which is unexpected e.g. granting and then revoking super user access within a short period of time.

5.3.2. The applicable manager, who is not a system and/or database administrator, must review the audit trail notifications on a weekly basis.

5.3.3. Anomalies must immediately be reported to appropriate management for follow-up action.

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