UNIVERSITEIT
STELLENBOSCH
UNIVERSITY

# Identity and Access Management Policy

| | |
|---|---|
| **Type of Document:** | Regulation |
| **Purpose:** | The policy establishes principles and provisions by which the identity, specifically the electronic identity, of natural persons who have a relationship with the Stellenbosch University as well as their access privileges are managed across the University. |
| **Approved by:** | Interim approval: Senior Director: IT (MW Dreijer) |
| **Date of Approval:** | 2012/12/01 |
| **Date of Implementation:** | 01/01/2013 |
| **Date of Next Revision:** | As required |
| **Date of Previous Revision(s):** | None |
| **Policy Owner[1]:** | Chair: Risk Management Committee |
| **Policy Curator[2]:** | Senior Director: Information Technology |
| **Keywords:** | Access Management, Identity Management, Electronic Identity |
| **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

# Identity and Access Management Policy

| | |
|---|---|
| **Reference number** | 0605-IAM Interim |
| **HEMIS Classification** | 0605 |
| **Purpose** | The policy establishes principles and provisions by which the identity, specifically the electronic identity, of natural persons who have a relationship with the Stellenbosch University as well as their access privileges are managed across the University. |
| **Date of implementation** | 1 December 2012 |
| **Review date** | |
| **Previous reviews** | |
| **Policy owner** | Chair of the Risk Management Committee |
| **Policy curator** | Senior Director: Information Technology |
| **Date of approval** | |
| **Approved by** | Interim approval: MW Dreijer, Senior Director: IT |

## 1. Purpose & Scope

The policy establishes principles and provisions by which the identity, specifically the electronic identity, of natural persons who have a relationship with the Stellenbosch University (hereafter “University”), as well as their access privileges are managed across the University. Identity and access management (IAM) is vitally important in ensuring that unauthorised electronic access to information, systems and physical areas, and potentially fraudulent activities are prevented.

IAM falls within the realm of information security management which aims to secure University information and information technology assets. As such it is a sub-policy of the *Information Security Regulation*.

The policy applies to the management of the electronic identity of all natural persons with whom the University maintains a relationship, including, but not limited to: students, staff, contractors, alumni, prospective students, parents of students, representatives of suppliers, service providers and debtors, research collaborators and visiting faculty.

This policy does not provide for the control of physical access to information and areas that are *not* mediated and facilitated by electronic means.

## 2. Definitions

Refer to the *IT policy definitions* document.

2.1. **IAM** is a set of technologies, processes and data required to manage the identities of people that have some relationship with (affiliated with) the University, whether internal or external, the lifecycle of that relationship and their access privileges to information and systems.

2.2. An **electronic identity** is a set of electronic information about a person that identifies that person uniquely. At the University it is at least a *single*, unique "US Number", but can include additional attributes such as a *single* username, password, fingerprint data, digital photograph, email address(es), etc.

2.3. For the purposes of this policy a person's **role** defines that person's access rights and privileges. A person can have more than one role and roles can be added or removed. More than one person can have a given role, and roles may be transferred between persons.

2.4. **Information curators** care for the University's information assets that are placed under their control. They are most often the senior and chief directors of support and administrative divisions.

2.5. The **Identity Vault** contains consolidated identity and access information (roles) for all users, from which the same information may be provisioned to other systems that also require it, and against which other systems may authenticate and authorise users. It is the single, consolidated directory.

2.6. **Directory** systems and services comprise the repositories that store the electronic identities, roles and security credentials of all persons affiliated with the University, and the authentication and authorisation services that are provided to information systems.

2.7. **Federated identity** is a solution to the IAM challenges presented by the trends of researchers and students increasingly collaborating across institutional borders and the sharing of information resources amongst institutions. Federated identity seeks to avoid the need to manage the electronic identities of people who are affiliated to other institutions while securely managing their access rights to local information and information systems.

2.8. **Single sign-on (SSO)** is an authentication method whereby a user signs on (logs on) to one information system and is consequently automatically signed on to other, independent information systems.

2.9. The **US Number**[1] is a unique 8-digit number that is permanently allocated to each person who has a relationship with the University and is a fundamental component of the electronic identity. The number can never be re-used.

2.10. **Users** are a subset of the set of natural persons who have an electronic identity at the University. A user is able to interact and transact with University information and information systems and is most often required to authenticate electronically in order to do so.

[1] This is sometimes referred to as the "UT Number" by some staff.

## 3. Policy Provisions

3.1. The Senior Director: IT is the information curator for the information contained within IAM's identity vault and associated IAM components. The IAM system is operated by the IT Division.

3.2. The IAM system includes at least the following sub-systems and components:

3.2.1. The identity vault;
3.2.2. The central, authoritative person record repository;
3.2.3. The software and processes that generate electronic identities;
3.2.4. All directory systems and services;
3.2.5. All authentication and password management systems;
3.2.6. All software and systems that provision and de-provision electronic identities, synchronise identity credentials (usernames and passwords) between systems and codify the rules relating to the above;
3.2.7. Federated identity processes and systems.

3.3. A person with a relationship with the University will have a *single* **electronic identity**.

3.4. A person's **role(s)** (as defined above) is **separate** from the person's electronic identity.

3.5. A person's identity must be **adequately validated** for the access privileges that that person will be granted by virtue of the role(s) assigned to him/her.

3.6. A regulation that sets down the procedures, by which identity is validated before an electronic identity is created and allocated to a person, will be implemented. It will bind all divisions and entities that "create identities" within information systems. One of its key aims will be to minimise the risk of creating duplicate electronic identities.

3.7. Where **duplicate** electronic identities have been created all reasonable steps will be taken to eliminate the duplicates as soon as they are discovered. De-duplication procedures will be implemented.

3.8. A register of **information curators** and the information and information systems for which they are the curators must be established and maintained. Information curators will be required to formally acknowledge and accept their curatorship.

3.9. IAM provides the tools and systems that enable information curators to manage and audit access rights to their information and systems. The management of access remains the responsibility of the information curators. The granting of access privileges is known as **authorisation**.

3.10. **Information curators have specific access management responsibilities** in relation to the information assets for which they are the curators. Curators:

3.10.1. Determine who is (or what roles are) granted access to which information and systems and when.
3.10.2. Classify data and information under their curatorship, according to the requirements of the *Information Management Policy*.
3.10.3. Manage the process of granting and revoking access to information under their curatorship.
3.10.4. Ensure that access controls and privileges are reviewed and audited annually.

3.11. The granting and revocation of access privileges, and all access transactions must be **auditable**.

3.12. Identities will be managed through the full **lifecycle** from identity creation, through provisioning and role changes to ultimate de-provisioning.

3.13. A person will be required to **authenticate** his/her identity in order to claim his/her access privileges. Such authentication will most often require the person to provide a secret password[2]. In order to ensure that strong passwords are created and used, the University will strive to implement "single sign-on" (SSO) across its information systems. Multi-factor[3] and biometric authentication may be adopted, where appropriate, to ensure higher levels of security.

## 4. Governance

### 4.1. Governance Structure

Changes to this policy will be initiated by the Risk Management Committee and/or 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 policy changes eventually approved by the Rector's Management Team and Council.

### 4.2. Ownership

The policy is owned by the chair of the Risk Management Committee.

### 4.3. Approval

All University policies must be approved by Council.

### 4.4. Implementation

It is the Senior Director: IT's responsibility to implement the policy, with the assistance of other information curators.

### 4.5. Review

Policy review will be initiated by the Risk Management Committee and/or the Information Security Management Committee as and when deemed necessary.

[2] The *Password Regulation* deals with the management and creation of passwords.

[3] There are 3 forms (or factors) of authentication, in ascending order of security: what you as a user *have* (a card or token); what you *know* (passwords); what you *are* (biometrics such as fingerprints). Multi-factor authentication would use two or more of these factors in combination in order to ensure a higher level of security.

### 4.6. Roles and Responsibilities

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