



UNIVERSITEIT•STELLENBOSCH•UNIVERSITY
jou kennisvenoot • your knowledge partner

Electronic Identity Validation Regulation

Reference number	0605-IDVAL
HEMIS Classification	0605
Purpose	It aims to ensure that a person's identity is validated before an electronic identity is created and allocated to that person so that the risk of creating duplicate electronic identities is minimised.
Date of implementation	13 December 2012
Review date	
Previous reviews	None
Regulation owner	Chair of the Information Security Management Committee
Regulation curator	Senior Director: Information Technology
Date of approval	13 December 2012
Approved by	MW Dreijer, Senior Director: IT

1. Purpose & Scope

The *Identity and Access Management (IAM) Policy* requires that “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 [Stellenbosch University] information systems. One of its key aims will be to minimise the risk of creating duplicate electronic identities.”

This is that regulation.

2. Definitions

- 2.1. Refer to the *Identity and Access Management (IAM) Policy* and the *IT policy definitions* document for relevant definitions of terminology as used in this regulation.
- 2.2. For the purposes of this regulation the Operator is the person authorised by the relevant Information Curator to use the functions that may create a new US Number or modify attributes related to a US Number.

3. Regulation

- 3.1. A natural person with a relationship with the university will be allocated a **single, unique US Number** (referred to as **USN** hereafter in this document) as a component of his or her **electronic identity**.
- 3.2. In order to minimise the possibility of more than one USN being allocated to one person, attributes that uniquely identify a person are required. The type and number of attributes required will differ between people with a South African Identity Number and those without.

- 3.3. When *one other duplicate USN* is identified during the process of creating a USN, simply abandon the transaction and use the existing USN.
- 3.4. In the cases where more than one other USNs are identified or a duplicate USN is identified *outside* the process of creating a new USN, the problem must be assumed to be complex and must be reported to the IT Service Desk immediately as a *Duplicate USN*. The Service Desk will log a pre-defined call and alert the appropriate section for action. Such duplicates will be managed on a case-by-case basis within a defined process with proper change management.
- 3.5. Identity validation for persons who possess a South African Identity Number

3.5.1. The following attributes for the person are required:

- a) **South African (SA) Identity Number.** This number must comply with the modulus as defined in [Addendum B](#). This number must be unique to the database. If it already exists the transaction may not proceed.
- b) Surname;
- c) First names;
- d) Initials;
- e) Date of birth;
- f) Gender.

3.5.2. If the action is a create (add):

- a) The above is the minimum data required to create a new USN. Should any of the above not be present the transaction may not proceed.
- b) The SA Identity Number is a unique identifier. If the SA Identity Number already exists on the database the transaction cannot proceed.
- c) Should the SA Identity Number not already exist on the database but the balance of the detail matches another record without an SA Identity Number, it is the responsibility of the Operator to resolve the possibility that this person already exists on the database without an SA Identity Number.

3.5.3. If the action is modify:

If the SA Identity Number is changed and the new number already exists on the database the transaction cannot proceed. This would indicate a duplicate USN and should be resolved as such. If any of the above detail is changed it is the responsibility of the “operator” to resolve the possibility that this person already exists on the database without an SA Identity Number.

- 3.6. Identity validation for persons who do *not* possess a South African Identity Number

3.6.1. The following attributes are required:

- a) Date of birth;
- b) Place of birth (city or town);
- c) Surname;
- d) First names;
- e) Initials;
- f) Gender;
- g) Nationality.

3.6.2. Roles

A person with a relationship with the university must have at least one role but may have many. Some roles (as listed in Addendum A) are required to conform to the requirements as set out under the section Business Requirements in document *BR.040*. This document is owned by the Human Resources (HR) Division. A copy of the document can be obtained from the HR Service Desk.

3.6.3. If the action is create (add):

- a) The above attributes are the minimum required to create a new USN. Should any of the above not be present the transaction may not proceed.
- b) If the role of the person requires it, detail specified in *BR.040* is required (see [Addendum A](#) for roles).

3.6.4. If the action is modify:

- a) If any of the above required attributes are changed it is the responsibility of the Operator to resolve the possibility that this person already exists on the database.
- b) If a role is changed or a new role added and the new role requires it, detail specified in *BR.040* is required (see [Addendum A](#) for roles).

4. Governance**4.1. 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 where necessary, before approving them.

4.2. Ownership

The regulation is owned by the chair of the Information Security Management Committee.

4.3. Approval

This regulation will be ratified by the Information Security Management Committee and approved by the Senior Director: IT.

4.4. Implementation

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

4.5. Review

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

4.6. Roles and Responsibilities**4.6.1. The Senior Director: IT**

The officer is responsible for maintaining and implementing the regulation.

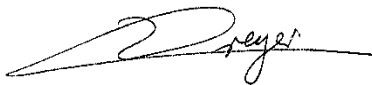
4.6.2. Information Curators and Operators

- a) Ensure that everything possible is done to prevent the creation of multiple USNs per person.
- b) Be aware of and use all possible aids and utilities to prevent the creation of multiple USNs per person.

4.6.3. Information Technology Division

- a) Create and modify software applications to prevent the creation of more than one USN per person.
- b) Write an audit line for each creation of an USN with at least the following attributes:
 - USN
 - Date
 - Time
 - Authorised user identity
- c) Enable an authorised user to identify possible duplicates by supplying utilities and validation procedures.
- d) Supply audit trails of all relevant transactions
- e) Make utilities available to identify existing or possible duplicates.

Approved by:



Mr Helmi Dreijer
Senior Director: Information Technology
Stellenbosch University

Addendum A

The table below indicates roles that require *BR.040* detail where the person does not possess a South African Identity Number:

Role
Student
Debtor
Creditor
Visitor
Staff member
Visiting faculty

Addendum B: SA Identity Number Modulus

Each South African citizen is required to have a 13-digit identity number. The SA Identity Number is also issued to permanent residents of SA. The validity of this number is determined using a modulus with the 13th digit, which is a check-digit (CD).

The modulus is as follows: (See ID number **5510135089** example below):

1. Calculate total **a** by adding the digits in odd positions (1, 3, 5, 7, 9, 11)
2. Calculate total **b** by using the digits in the even positions (2, 4, 6, 8, 10, 12) as an integer which is multiplied by 2;
3. Now add the digits of the product in point 2.
4. Calculate total **c** by adding total **a** and total **b**;
5. The check digit is calculated by subtracting the last digit of the units of **c** from 10. NOTE: If total **c** is a multiple of 10 the check digit will be 0.

If the new CD does not match the 13th digit of the original identity number, the number is invalid;

If the identity number is found to be not invalid in the preceding step, the 11th digit of the original identity number must be 0 or 1, else it is invalid;

If the identity number is found to be not invalid in the preceding step, the 12th digit must be an 8 or 9. If the 12th digit is neither it must be replaced with an 8.

Recalculate the CD for this new number up to step 5.

Replace the 13th digit with the CD.

The resulting, converted identity number is stored in the database.

Example: ID Number 5510135089087

Position	1	2	3	4	5	6	7	8	9	10	11	12	13
ID Number	5	5	1	0	1	3	5	0	8	9	0	8	7

1. $5+1+1+5+8+0 = 20$ – (Total **a**: sum of digits in odd positions);
2. $503098*2 = 1006196$ – (even positions as integer * 2) ;
3. $1+0+0+6+1+9+6 = 23$ – (Total **b**: Sum of product in step 2);
4. $20+23=43$ – (Total **c**: Sum of total **a** and **b**);
5. $10 - 3 = 7$ = to last digit of ID number & therefore valid