



UNIVERSITEIT  
STELLENBOSCH  
UNIVERSITY

## Records Management Policy

<b>Type of Document:</b>	Policy
<b>Purpose:</b>	To maintain, protect, retain and dispose of records in accordance with fiscal, legal and historical requirements.
<b>Approved by:</b>	SU Council
<b>Date of Approval:</b>	2016/11/28
<b>Date of Implementation:</b>	2017/01/01
<b>Date of Next Revision:</b>	2021
<b>Date of Previous Revision(s):</b>	Every five years
<b>Policy Owner<sup>1</sup>:</b>	Registrar
<b>Policy Curator<sup>2</sup>:</b>	Records Manager
<b>Keywords:</b>	Records, Records Management, Retention, Disposition, Governance, Records Management Principles
<b>Validity:</b>	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](http://www.sun.ac.za/policies)

---

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

<sup>2</sup> Policy Curator: Administrative head of the division responsible for the implementation and maintenance of the policy



## 1. Introduction

---

Stellenbosch University, here after SU, has a records management program that maintains, protects, retains, and disposes of records in accordance with operational needs, governmental regulations, adopted international standards, fiscal and / or legal requirements, historical, and reference purposes. All records in all formats and in all locations of SU are managed in accordance with this policy. Records Management may or may not include information from other information sources, e.g. data systems, content management systems, knowledge management systems and business information systems.

There is a subtle difference between data and information. Data are the facts or details from which information (records and documents) is derived. Individual pieces of data are rarely useful alone. For data to become information, data needs to be put into context.

This Records Management Policy is not intended to be comprehensive in all respects, but forms part of SU's integrated management model and should be read in conjunction with the University's other policies, including the SU Policy for Responsible Research Conduct (2013), SU Policy on Mandatory Self-archiving of Research Output (2014) and the SU Policy in Respect of Exploitation of Intellectual Property (2010).

## 2. Intent

---

The intent of this policy is to:

- 2.1 Enable SU to meet all the legal obligations stemming from the relevant South African legislation governing information and records management.
- 2.2 Provide the foundation for defining the principles governing records management at SU.
- 2.3 Support SU's institutional governance ethics and processes by a comprehensive and viable set of requirements regarding records management.
- 2.4 Support SU in its vision to be innovative and future focused and to ensure systemic sustainability of the organisation.
- 2.5 Implement new and standardized working methods for storing, retrieving and retaining records.

## 3 Scope

---

This policy applies to electronic, multi-media and hard copy records in all formats created, received, managed, stored, retained and disposed by SU. It includes all institutional, commercial and technical records relevant to the work of SU. Controlled Records and Institutional Documents are both covered by this Policy. Retention and destruction of SU records are in accordance with the approved SU Records Retention Schedule.

## 4 Application

---

This policy is applicable to all institutional functions within SU. As a result, this policy is applicable to all employees, contractors, consultants and students who manage, view or create electronic and physical records, including documents and any associated data or information, in all formats and on all media.

Any reference to records in this policy, and its appendices, is a reference to records and documents created, received, and maintained. These serve as evidence of transactional activities by the institution or person, in pursuance of legal obligations or in the execution of responsibilities. Access will be granted in accordance with the Identity and Access Management Policy of SU, (2012).

---

### Stellenbosch University – Internal Use Only

This document may contain proprietary and/or confidential information. This document is a controlled document. The controlled copy is maintained electronically by the SUNREKORDS Function. Any printed copy of this document is an uncontrolled copy



---

## 5 Confidentiality and Non-disclosure of Records

---

Employees, contractors, consultants and students may not disclose the nature and contents of any record to any person unless such disclosure is permitted in terms of the employee's job description, contract of employment or upon written authorization from the Records Manager in consultation with Legal Services.

## 6 Integrity

---

- 6.1 All records will be identified, classified, retained, stored and protected in such a manner that their integrity is not compromised.
- 6.2 Stringent guidelines and procedures must ensure that records are admissible evidence in courts or disciplinary proceedings notwithstanding the fact that such records were created, distributed or stored in electronic format.
- 6.3 Scanning of records from paper into an electronic format must be conducted in such a way that digital images can be proven to be an authentic copy of the original.

## 7 Duty of Care

---

SU has a duty to keep secure and accurate original records or authentic copies of them. This is achieved by all employees, contractors, consultants and students.

## 8 Records Management Realisation

---

SU will define, plan and implement the processes that are required to realise the required quality of records management as well as the sequence and interaction of these processes. SU will ensure that these processes are operated under controlled conditions and produce outputs, which meet customer requirements. This policy requires that the implementation thereof is assigned to the office of the Records Manager.

## 9 Policy Governance

---

The Records Management Policy will be governed by appropriate structures within SU.

## 10 Audit

---

- 10.1 Records Management audits will be undertaken on a regular basis.
- 10.2 The following audit types, but not limited to these, will be conducted:
  - 10.2.1 Access and Security Audit
  - 10.2.2 Storage Areas Audit
  - 10.2.3 Physical and Electronic Filing Audit
  - 10.2.4 Disposal Audit

## 11 Revision

---

This policy is part of a wider set of documents related to Records Management within SU (see Annexure B). To assist in the sustainability and continuous improvement of records management practices, this policy and the related procedures shall be reviewed at least every 5 years, or sooner, depending on compelling interim amendments, and published with approved changes.



## Annexure A: Glossary

Term	Definition <sup>1</sup>
Accurate Original Records <sup>2</sup>	Accurate Original Records are records that truly reflect the transaction they document, serves the purpose they are kept for, provide evidence that they actually are what they purport to be and are properly secured to prevent unauthorised access, alteration or removal.
Controlled Records	Controlled records are institutional records that have gone through a formal process of approval. This includes standardisation and approval of all templates used within the Institution, e.g. Claim Forms, Leave Forms, Minutes of Meetings, etc. Other types of controlled documents are Policies, Procedures, Regulations, Standards, etc. that go through a lifecycle of, "draft, review, approved and published" (an ISO standard). The annual or 2, or 5 yearly review of policies for example, will follow the same lifecycle of review, approval and then only publication for use of viewing by the Institution.
Data	Data is raw, unorganized facts that need to be processed. Data can be something simple and seemingly random and useless until it is organized.
Destruction	The process of eliminating records beyond any physical reconstruction.
Disposal	Disposal is the action taken when: <ul style="list-style-type: none"> <li>• records with vital or historical value are archived, and</li> <li>• ephemeral (non-archival) records are destroyed/deleted.</li> </ul>
Electronic Record	A record (excluding data sources) that is generated electronically and stored by means of computer technology
Evidence	All information that is presented to solve a problem and serve as grounds for the final decision.
Format	The physical form, such as paper, photographs, microfilm, sound recording, machine readable electronic record or other material, or computer file format in which a record is maintained.
Governance	The framework of rules and practices by which a board of directors ensures accountability, fairness, and transparency in a company's relationship with all its stakeholders (financiers, customers, management, employees, government, and the community).
Institutional Activities	The major activities performed by an institution to accomplish each of its functions.
Institutional Documents	Institutional documents are all institutional related documents, other than controlled records, that are used for the daily communication and evidence of transactions performed in the undertaking of all departmental activities. Institutional documents range from brief email messages to complex legal agreements. Some documents are prepared by employees and business owners, while others are drafted

<sup>1</sup> Insiq: records management programme. The nuts and bolts of records management, 2 June 2011: participant workbook / North-West University.

<sup>2</sup> (<http://www.businessdictionary.com/definition/full-and-accurate-record.html>)  
[http://www.diffen.com/difference/Data\\_vs\\_Information](http://www.diffen.com/difference/Data_vs_Information)



	by professionals from outside of the company, such as accountants and lawyers.
Institutional Functions	Institutional Functions are a general description of operations performed regularly to carry out the institution's mission. In Records Management institutional functions are not necessarily departments as per the organizational structure of an organization or institution. Multiple institutional functions can be performed in one single department.
Institutional Process	Set of interrelated or interacting activities, performed by institutional entities, that transform inputs into outputs.
Legal Obligation	Compliance with legislation.
Record	A record is something which is generated by an institutional activity, including but not limited to research information, data and activities, as part of an institutional process, and often in pursuance of legal obligation, and its existence is evidence of the fact that the activity or process took place.
Records Management Programme	A records management programme is the systematic and consistent control of all records throughout their lifecycle.
Retention	Retention indicates how long the records have to be kept before the disposal action is undertaken.
Retention Schedule	A report identifying the approved retention periods for records of an organisation. It establishes a time table, regulating the lifecycle of records in the office from creation to their final disposition, whether they will be destroyed or transferred to the archives or archived electronically.
Vital Records	Records without which the organisation cannot continue to operate. These records protect the assets and interests of the organisation.



## Annexure B: Related Documents

---

1. Basic Conditions of Employment Act, no 75 of 1997 (all amendments and revisions).
2. Compensation for Occupational Injuries and Diseases Act, no. 130 of 1993 (all amendments and revisions).
3. Directive issued in terms of the Public Audit Act, no. 25 of 2004 (all amendments and revisions).
4. Electronic Communications and Transactions Act, no. 25 of 2002 (all amendments and revisions).
5. Higher Education Act, no. 101 of 1997. (all amendments and revisions).
6. International Standards for Information and Documentation – Records Management Part 1: General (ISO 15489-1) 2001 20.
7. International Standards for Information and Documentation – Records Management Part 2: Guideline (ISO 15489-2) 2001 21.
8. IT Services Standard Data Storage Security University of Lethbridge 2015\_04\_17.
9. National Archives and Records Services of South Africa Act , no. 43 of 1996 (all amendments and revisions).
10. National Archives and Records Services of South Africa Regulations (2002), Regulation R158 (all amendments and revisions).
11. POPI Privacy Prioritisation: Stellenbosch University 30 August 2013.
12. Promotion of Access to Information Act, no. 2 of 2000 (PAIA) (all amendments and revisions).
13. Promotion of Administrative Justice Act, no. 3 of 2000 (PAJA) (all amendments and revisions).
14. Public Audit Act, no.25 of 2004 (all amendments and revisions).
15. Records Management Procedures:
  - 15.1 Retention Schedule & Disposition Procedure (PRO-001-RRD\_2016)
  - 15.2 Access & Security Procedure (PRO-002-ACSE\_2016)
  - 15.3 Records Hold Procedure (PRO-003-HOLD\_2016)
  - 15.4 Records Classification and Identification (PRO-004-RMCIP\_2016)
  - 15.5 Records Change Control Procedure (PRO-005-CHC\_2016)
  - 15.6 Records Management Audit Procedure (PRO-006-RMAUD\_2016)
  - 15.7 Records Management Storage and Disposal Procedure (PRO-007-SDP\_2016)
  - 15.8 Vital Records Protection Procedure (PRO-008-VIT\_2016)
  - 15.9 Records Management Scanning and Imaging Procedure (PRO-009-SCI\_2016)
16. Records Management Strategy, 2016.
17. Regulation of Interception of Communications Act, no. 70 of 2002 (all amendments and revisions).
18. SAICA Guide on the Retention of Records April 2016.
19. South African National Board Standards for Electronic Imaging - Information Stored Electronically – Recommendations for Trustworthiness and Reliability (SANS 15801).
20. South African National Board Standards for Information and Documentation – Records Management Part 1: General (SANS 15489-1) 2004 22.
21. South African National Board Standards for Information and Documentation – Records Management Part 2: Guideline (SANS 15489-2) 2004.



22. South African National Board Standards for Information and Documentation – Records Management Processes – Metadata for Records Part 1: Principles (SANS 23081).
23. South African National Board Standards for Information Technology – Security Techniques – Code of Practice for Information Security Management (SANS 17799).
24. South African Qualifications Authority Act, no. 58 of 1995 (all amendments and revisions).
25. Stellenbosch University Information Management Policy (draft).
26. Stellenbosch University Information Security Regulations, 2010.
27. Stellenbosch University Institutional Intent and Strategy 2013-2018.
28. Stellenbosch University PAIA Manual.
29. Stellenbosch University Policy for Responsible Research Conduct, 2013.
30. Stellenbosch University Policy in Respect of Exploitation of Intellectual Property, 2010.
31. Stellenbosch University Policy on Mandatory Self-archiving of Research Output, 2014.
32. Tax Administration Act, no. 28 of 2011 (all amendments and revisions).