NWU Policy and Rules on Data and Information Security

Reference number	1P_1.16.1_a
Accountable executive manager	Registrar
Policy Owner	Registrar
Responsible division	Office of the Registrar
Status	Approved
Approved by	Council
Date of approval	23 June 2022
Date of amendments	
Review date	2025

Office of the Registrar

NWU POLICY AND RULES ON DATA AND INFORMATION SECURITY

Preamble

Against the background of the dream to be an internationally recognised university in Africa, distinguished for engaged scholarship, social responsiveness and an ethic of care, the Council of the North-West University (NWU) has adopted the Policy and rules on Data and Information Security on 23 June 2022.

1 Interpretation and application

This policy must be interpreted and applied in a manner consistent with the –

1.1 Constitution of the Republic of South Africa, 1996;

1.2 Higher Education Act, 101 of 1997;

1.3 Protection of Personal Information Act, 4 of 2013 ("POPIA");

1.4 Promotion of Access to Information Act, 2 of 2000 ("PAIA");

1.5 King IV Report on Good Corporate Governance in South Africa;

1.6 POPIA Industry Code of Conduct: Public Universities (USAf, June 2020);

1.7 Statute of the North-West University ("the Statute");

1.8 Information Governance Framework of the NWU;

1.9 NWU Risk Management Policy;

1.10 NWU Business Continuity Policy;

1.11 NWU IT Governance Policy;

1.12 NWU IT Fair Use Policy; and

1.13 Rules and Guidelines relevant to IT and information security as these are published from time to time by the University.

2 Definitions

In this policy –

"data" means the representation of facts, concepts or instructions in a formal manner, suitable for communication, interpretation or processing by human or by automatic means; and

"information" means knowledge concerning objects such as facts, events, things, processes or ideas, including concepts that have a particular meaning within a certain context.

3 Policy statement

3.1 The NWU views data and information security to be of paramount importance for the good governance and effective and efficient management and administration of the university.

3.2 The rules set out in paragraph 5 are adopted in order to maintain the data and information security of the university against all threats.

4 Scope of application

This policy and the rules set out in paragraph 5 apply to security measures in the generation, management and maintenance of all kinds of data and information at the NWU as these take place in all business processes and by all members of the NWU, its suppliers and service providers.

5 Rules on data and information security

5.1 For the purposes of the implementation of an overall and uniform data and information security management system, the following overarching goals must be pursued:

5.1.1 the development and maintenance of a detailed data and information systems inventory, containing complete information on all the IT systems utilised at the NWU;

5.1.2 the categorization of data and information systems in respect of levels of confidentiality, integrity and availability, each rated in accordance with the sensitivity of data it contains and with respect to requisite security measures needed to protect the data and information from being compromised, and

5.1.3 the management of data and information security in a proactive manner in order to curb risks, challenges and threats in the institutional network such as internal and external cyber attacks and system malfunctioning and loss of data.

5.2 A governance and management environment conducive to the implementation of information security controls safeguarding the NWU's data and its information assets must be established and maintained –

5.2.1 by means of a systematic and ongoing examination of data and information security risks relevant to higher education in general and the NWU in particular, taking into account external threats, inherent vulnerabilities and the impact of risks relevant to data and information security;

5.2.2 by developing and maintaining a system security plan detailing risks relevant to data and information security, the requisite controls and assurance provisioning, including security planning by means of a comprehensive quality management approach, departing from the Plan-Do-Check-Act model so as to ensure sufficient coverage of the security management lifecycle:

- Plan: documented guidelines, procedures relevant to security objectives, roadmaps to achieve these, including monitoring mechanisms and responsibility matrices.
- Do: implementation of security controls.
- Check: performance of tests to determine that controls are operating as intended and that these meet the requisite objectives.
- Act: Remediation of gaps and deficiencies.

5.2.3 by establishing a configuration-management environment for the purpose of providing a complete understanding of the NWU's data and information landscape in terms of its network devices, operating systems, applications, externally and internally developed services, systems, hardware and software platforms in order to establish, maintain, record and monitor the security of these configurations.

5.2.4 By ensuring system-, data- and information integrity by the establishment of relevant measures including those related to malware, application and source code flaws, security alerts advisories and directives, spam protection, information-input validation, as well as the remediation of detected and disclosed integrity issues;

5.2.5 By implementing and managing controls before, during and after a contractual relationship between the NWU and any individual or party;

5.2.6 By implementing an incident-response structure plan to ensure appropriate responses and ongoing improvement at levels where data and information security incidents take place, indicating the following at the relevant level of operation:

- the responsibility matrix
- procedures to be implemented
- response and recovery time to incidents
- evidence
- learning from incident

5.2.7 by means of the identification od and authentication regarding aspects relevant to ensuring readiness, performance, design and implementation of security measures for business operations as well as in regard to business continuity;

5.2.8 by managing access control to data and information and physical locations, i.e. the provision of guidelines and procedures defining digital and physical permission restrictions in regard to matters related to data and information classification in accordance with paragraph 5.1.2, and in accordance with the NWU File plan;

5.2.9 by managing access rights to physical spaces as well as access control to networks and network services;

5.2.10 by implementing awareness and training programmes aimed at the relevant internal and external stakeholders on matters relevant to data and information security, the implementation of this policy, and by taking practical measures demonstrating the effectiveness and efficiency of the information security measures;

5.2.11 by implementing an overarching business continuity framework plan consisting of a suite of plans, procedures, technical requirements, and initiatives for ensuring recovery of information systems, operations, data and information in all instances of disruption or relevant services;

5.2.12 by continuously -monitoring and reporting on information security performance and related processes including controls having the purpose of ensuring continuous quality enhancement and maturity levels, determining, amongst others, the following:

5.2.12.1 business processes and results that could be affected by variations in terms of information security performance, including the controls relevant in such environments, as well as relevant instances of regulatory and directive governance; and

5.2.12.2 methods to be used for purposes of measurement in the relevant environment (including manual, mechanical, software) so as to ensure verifiable and repeatable results

5.2.13 by providing assurance on the appropriateness, the effectiveness and efficiency of information security controls that safeguard the University's data and information assets; and

5.2.14 by providing evidence and reports drafted for audit-trail, management and governance purposes.

6 Roles, responsibilities and accountability

6.1 The council is accountable and takes responsibility for the establishment of an environment conducive to the governance of effective and efficient data and information security management.

6.2 The council is advised by the Technology and Information Governance Committee (TIGovCom) on the manner in which this policy is implemented, on the appropriateness of the guidelines, rules, procedures and protocols in respect of the NWU's data and information security management system and the effectiveness of the management of relevant risks.

6.3 The University Management Committee (UMC) is responsible for the establishment of a management environment to ensure data and information security in all business processes and for achieving the management objectives set by council in accordance with this policy.

6.4 The UMC must –

6.4.1 promote a culture embedding data and information security in all relevant business processes;

6.4.2 establish guidelines, rules, standards and procedures in respect of an overarching NWU data and information security management system;

6.4.3 ensure the implementation of a programme to ensure ongoing awareness and training of all internal stakeholders in matters relevant to data and information security; and

6.4.4 report on the effectiveness and efficiency of the implementation of the NWU's data and information security management system to the TIGovCom.

6.5 In relation to the ongoing management of matters related to data and information security, the Information Management Committee (IMCom) and the Information Technology Committee (ITCom) receive reports from the Registrar's portfolio and from the Chief Director IT and advise the UMC on the effective and efficient management of data and information security in accordance with this policy.

Original details: (11664754) P:\Policies\2022\1P_1.16.1_a\NWU Policy and Rules on Data and Information Security.docm
27 June 2022

File reference: 1P_1.16.1A