DRAFT SECURITY POLICY

 OF THE

 UNIVERSITY OF VENDA

CONTENTS

1. PREAMBLE
2. PURPOSE
3. OBJECTIVES
4. SCOPE
5. PRINCIPLES
6. LEGISLATIVE AND REGULATORY REQUIREMENTS
7. POLICY STATEMENT
8. SPECIFIC RESPONSIBILITIES
9. AUDIENCE
10. ENFORCEMENT
11. EXCEPTIONS
12. OTHER CONSIDERATIONS
13. COMMUNICATING THE POLICY
14. REVIEW AND UPDATES
15. IMPLEMENTATION
16. MONITORING COMPLIANCE
17. DISCIPLINARY ACTION
18. GLOSSARY

 **POLICY ON SECURITY**

1. **PREAMBLE**

The University of Venda is committed to providing a secure campus environment where people are safe, assets are protected and teaching, and learning and research activities are conducted unhindered.

1. **PURPOSE**
	1. The University of Venda depends on its personnel, information and assets to deliver services that ensure the health, safety, security and economic wellbeing of South African citizens. It must therefore manage these resources with due diligence and take appropriate measures to protect them.
	2. Threat that can cause harm to the university of Venda , in South Africa and abroad, include acts of terror and sabotage, espionage, unauthorised access to buildings and premises, theft, armed robbery, fraud and corruption, vandalism, fire, natural disasters, technical failures and accidental damage. The threat of cyber attack and malicious activity through the internet is prevalent. Threat to the national interest, such as transitional criminal activity, foreign intelligence activities and terrorism, continue to evolve as the results of changes in the international environment.
	3. The Security policy of the University of Venda prescribes the application of security measures to reduce the risk of harm that can be caused to the institution if the above threat should materialize. It has been designed to protect employees, preserve the confidentiality, integrity, availability and value of information and assets, and assure the continued delivery of service. Since the University of Venda relies extensively on information and communication technology (ICT) to provide its services, this policy emphasizes the need for acceptable use of ICT equipment as well as ICT Protection measures to be complied with by the employees.
	4. The main objective of this policy therefore is to support the national interest and the University of Venda business objectives by protecting employees, information and assets and assuring the continued delivery of services to South African Citizens.
	5. The policy complements other University of Venda’s polices (e.g. sexual harassment, occupational health and safety, official languages, information management, asset control, real property and financial resources).
2. **OBJECTIVES**

The main objectives of the policy are to:

* 1. Minimise the risk and fear of falling the victim of crime.
	2. Promote an individual and collective sense of responsibility towards security of all people on campus, all university infrastructure and all assets.
	3. To protect all assets against theft, loss or damage.
1. **SCOPE**
	1. The policy applies to the following individuals and entities:
* All employees of the University of Venda
* All contractors and consultants delivering a service to the University of Venda including their employees who may interact with the University of Venda.
* Temporary employees of the University of Venda
* All information assets of the University of Venda
* All intellectual property of the University of Venda
* All fixed property that is owned or leased by the University of Venda
* All moveable property that is owned or leased by the University of Venda.
	1. The policy further covers the following seven elements of the security program of the University of Venda
* Security organization
* Security administration
* Information security
* Physical security
* Personnel security
* Information and Communication Technology (ICT) security
* Business continuity Plan (BCP).
1. **PRINCIPLES**
	1. The security and protection of all people is a priority to University Management.
	2. All security is the responsibility of every individual of the campus community. Responsible behaviour is required from all members of the University community and developed through a sense of awareness and strong will to protect University property. In order to maintain an effective security system, the university requires the cooperation of every employee.
	3. All staff in managerial or supervisory positions and student leaders must be aware of security risks and implement the necessary security measures in his/her work environment.
	4. All security related incidents shall be reported to protection services.
	5. The person in control of the University assets that are stolen or damaged shall report the crime to the nearest police station.
	6. All crimes committed on University premises shall be reported to the South African Police Services.
2. **LEGISLATIVE AND REGULATORY REQUIREMENTS**
	1. This policy is informed by and complies with applicable national legislation, national security policies and national security standards. A list of applicable regulatory documents in this regard are listed below:

Applicable legislations

* Constitution of the Republic of South Africa, 1996 (Act 106 of 1996)
* Protection of information Act, 1982 (Act no 84 of 1982)
* Promotion of Access to information Act,2000 (Act 2 of 2000)
* Promotion of Administrative Justice Act, (Act 3 of 2000)
* Copyright Act, (Act 98 of 1978)
* National Archives of South Africa Act, 1996 (Act no 43 of 1996) and regulations
* Public Service Act, 1994 (Act no 103 of 1994) and regulations
* Occupational Health and Safety Act, 1993 (Act no 85 of 1993)
* Criminal Procedure Act, 1997 (Act no 51 of 1977)
* Private Security Industry Regulations Act, 2001 (Act 56 of 2001)
* Control of Access to Public Premises and Vehicles Act, 1985 (Act 53 of 1985)
* National Key Points Act, 1980 (Act 102 of 1980)
* Trespass Act, 1959 (Act 6 of 1959)
* Electronic Communication and Transaction Act, 2002 (Act 25 of 2002)
* Electronic Communications Security (Pty) Ltd Act, 2002 (Act 68 of 2002)
* State Information Technology Agency Act, 1998 (Act 88 of 1998)
* Regulation of Interception of Communications and Provision of Communication related Information Act, 2002 (Act 70 of 2002)
* General Intelligence Law Amendment Act, 2000 ( Act 66 of 2000)
* Intelligence Service Act, 2002 (Act 65 of 2002) and regulations
* National Strategic Intelligence Act, 1994 (Act 39 of 1994)
* Intelligence Service Control Act, 1994 (Act 40 of 1994)
* Labour Relations Act, 1995 ( Act 66 of 1995)
* Employment Equity Act, 1998 ( Act 55 of 1998)
* Occupational Health and Safety Act , 1993 (Act 85 of 1993)
* Fire Arm Control Act, 2000 (Act 60 of 2000) and regulations
* Non-Proliferation of Weapons of Mass Destruction Act, 1993 (Act 87 of 1993)
* Protection of Constitutional Democracy Against Terrorism and Related Activities Act, 2004 (Act 33 of 2004)
* National Building Regulations and Building Standards Act, 1977 (Act 103 of 1977)
* Protected Disclosures Act, 2000 (Act 26 of 2000)
* Intimidation Act,1982 (Act 72 of 1982)
* Prevention and Combating of Corrupt Activities Act,2004 (Act 12 of 2004)
* Public Finance management Act, 1999 (Act 1 of 1999) and Treasury Regulations
1. **POLICY STATEMENT**

7.1. **General**

* Employees of the University of Venda must be protected against identified threats according to baseline security requirements and continuous security risk management.
* Information and assets of the University of Venda must be protected according to baseline security requirements and continuous security management.
* Continued delivery of services of the University of Venda must be assured through baseline security requirements, including business continuity planning, and continuous risk management.

7.2. **Compliance Requirements**

7.2.1. All individuals mentioned in par. 4 above must comply with the baseline requirements of this policy and its associated Security Directives as contained in the Security Plan of the University of Venda. These requirements are/shall be based on the on integrated security Threat and Risk Assessments (TRA’s) to the national interest as well as employees, information and assets of the University of Venda. The necessity of security measures above baseline levels will also be determined by the continual updating of a security Threat and Risk Assessments.

7.2.2. **Security Threat and Risk Assessments involve:**

* Establishing the scope of the assessment and identifying the information, employees and assets to be protected;
* Determining the threats to information, employees and assets of the University of Venda and assessing the probability and impact of threat and occurrences;
* Assessing the risk based on the adequacy of existing security measures and vulnerabilities:
* Implementing any supplementary security measures that will reduce the risk to acceptable levels.

7.2.3**. Staff accountability and acceptable use of assets**

7.2.3.1. The Principal of the University of Venda shall ensure that information and assets of the University of Venda are used in accordance with the procedures as stipulated in the Security Directives as contained in the Security Plan of the University of Venda.

7.2.3.2. All employees of the University of Venda shall be accountable for the proper utilisation and protection of such information and assets. Employees that misuse or abuse assets of the University of Venda shall be held accountable therefore and disciplinary action shall be taken against any such employee.

7.3. **Specific baseline requirements**

7.3.1. **Security organisation**

7.3.1.1. The Principal of the University of Venda will appoint / has appointed a Director to establish and direct a security program that ensures coordination of all policy functions and implementation of policy requirements.

7.3.1.2. Given the importance of this role, a Director with sufficient Campus security experience and training who is strategically positioned within the University of Venda so as to provide institution-wide strategic advice and guidance to senior management has been/will be appointed.

7.3.1.3. The Principal of the University of Venda will ensure that the Security Director has an effective support structure (security component) to fulfil the functions referred to in par 7.3.2 below.

7.3.1.4. Individuals that will be appointed in the support structure of the Director will all be security professionals with sufficient security experience and training to effectively cope with their respective job functions.

7.3.2. **Security Administration**

7.3.2.1. The functions referred to in par 7.3.1 above include:

* General security administration (departmental directives and procedures, training and awareness, security risk management, security audits, sharing of information and assets);
* Setting access limitations:
* Administration of security screening:
* Implementing physical security;
* Ensuring the protection of employees;
* Ensuring the protection of information;
* Ensuring ICT security;
* Ensuring security in emergency and increased threat situations;
* Facilitating business continuity planning;
* Ensuring security in contracting; and
* Facilitating security breach reporting and investigations.

7.3.2.2. **Security incident/breaches reporting process**

7.3.2.2.1. Whenever an employee of the University of Venda becomes aware of an incident that might constitute a security breach or an unauthorised disclosure of information (whether or accidentally or intentionally), he/she shall report that to the Director of the University of Venda by utilizing the formal reporting procedure prescribed in the Security Breach Directive of the University of Venda.

7.3.2.2.2. The Principal of the University of Venda shall report to the appropriate authority (as indicated in the Security Breach Directive of the University of Venda) all cases or suspected cases of security breaches, for investigation.

7.3.2.2.3. The Director of Security of the University of Venda shall ensure that all employees are informed about the procedure of reporting security breaches.

7.3.2.3. Security incident/breaches response process

7.3.2.3.1. The Director Security shall develop and implement security breach response mechanisms for the University of Venda in order to address all security breaches/alleged breaches which are reported.

7.3.2.3.2. The Director Security shall ensure that the Principal of the University of Venda is advised of such incidents as soon as possible.

7.3.2.3.3. It shall be the responsibility of the National Intelligence Structures (e.g. NIA or SAPS) to conduct an investigation on reported security breaches and provide feedback with recommendation to the University of Venda.

7.3.2.3.4. Access privileges to classified information. Assets and /or to premises maybe suspended by the Principal of the University of Venda until administrative, disciplinary and /or criminal process have been concluded, flowing from investigations into security breaches or alleged security breaches.

7.3.2.3.5. The end result of these investigations, disciplinary action or criminal prosecutions may be taken into consideration by the Principal of the University of Venda in determining whether to restore, or limit, the security access privileges of an individual or whether to revoke or alter the security clearance f an individual.

7.3.3. **Information security**

7.3.3.1. Categorization of information and information classification system

7.3.3.2. The Director must ensure that a comprehensive information classification system is developed for and implemented in the University of Venda. All sensitive information produced or processed by the University of Venda must be identified, categorized and classified according to the origin to its source and contents and according to its sensitivity to loss or disclosure.

7.3.3.4. Employees of the University of Venda who generates sensitive information are responsible for determining information classification thereof, subject to management review. This responsibility includes the labelling of classified documents.

7.3.3.5. The classification assigned to documents must be strictly adhered to and the prescribed security measures to protect such documents must be applied at all times.

7.3.3.6. Access to classified information will be determined by the following principles:

* Intrinsic secrecy approach
* Need-to-know
* Level of security clearance.

7.3.4. Physical Security

7.3.4.1. Physical security involves the proper layout and design of facilities of the University of Venda and the use of the security measures to delay and prevent unauthorized access to assets of the University of Venda. It includes measures to detect attempted or actual unauthorized access and the activation of an appropriate response. Physical security also includes the provision of measure to protect employees from bodily harm.

7.3.4.2. Physical security measures must be developed implemented and maintained in order to ensure that the entire University of Venda, its personnel, property and information are secured. These security measures shall be based on the findings of the Threat and Risk Assessment (TRA) to be conducted by the Security Manger.

7.3.4.3. The University of Venda shall ensure that physical security is fully integrated early in the process of planning, selecting, designing and modifying of its facilities. The University of Venda shall:

* Select, design and modify facilities in order to facilitate the effective control of access thereto;
* Demarcate restricted access areas and have the necessary entry barriers, security systems and equipment to effectively control access thereto;
* Include the necessary specifications in planning, request for proposals and tender documentation;
* Incorporate related costs in funding requirements for implementation of the above.

7.3.4.4. The University of Venda will also ensure the implementation of appropriate physical security measures for the secure storage, transmittal and disposal of classified and protected information in all forms.

7.3.4.5. All employees are required to comply with access control procedures of the University of Venda at all times. This includes the producing of ID Cards upon entering any sites of the University of Venda, the display thereof whilst on the premises and the escorting of official visitors.

7.3.5.1**. IT Security**

7.3.6.1.1. A secure network shall be established for the University of Venda in order to ensure that information systems are secured against rapidly evolving threats that have the potential to impact on their confidentiality, integrity, availability, intended use and value.

7.3.6.1.2. To prevent the compromise of IT systems, the University of Venda shall implement baseline security controls and any additional control identified through the security Threat and Risk Assessment (TRA). These controls, and the security roles and responsibilities of all personnel, shall be clearly defined, documented and communicated to all employees.

7.3.6.1.3. To ensure policy compliance, the ICT Director of the University of Venda shall:

* Certify that all IT systems are secured after procurement, accredit IT systems prior to operation and comply with minimum security standards and directives;
* Conduct periodic security evaluations of systems, including assessments of configuration changes conducted on a routine basis;

7.3.6.1.4. Server rooms and other related security zones where IT equipment are kept shall be secured with adequate physical security measures and strict access control shall be enforced and monitored.

7.3.6.1.5. Access to resources on the network of the University of Venda shall be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals of the University of Venda shall be restricted unless explicitly authorized.

7.3.6.1.6. System hardware, operating and application software, the network and communication systems of the University of Venda shall be adequately configured and safeguarded against both physical attack and unauthorized network intrusion.

7.3.6.1.7. All employees shall make use of IT systems of the University of Venda in an acceptable manner and for business purposes only. All employees shall comply with the IT Security Directives in this regard at all times.

7.3.6.1.8. The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines as reflected in the IT Security Directives. In particular, passwords shall not be shared with any other person for any reason.

7.3.6.1.9. To ensure the ongoing availability of critical services, the University of Venda shall develop IT continuity plans as part of its overall Business Continuity Planning (BCP) and recovery activities.

7.3.6.2. Internet access

7.3.6.2.1. The Director: ICT of the University of Venda, having the overall responsibility for setting up internet access for the University of Venda, shall ensure that the network of the University of Venda is safeguarded from malicious external intrusion by developing, as a minimum, a configured firewall. Human Resources management shall ensure that all personnel with internet access (including e-mail) are aware of, and will comply with, an acceptable code of conduct in their usage of the internet.

7.3.6.2.2. The ICT Director of the University of Venda shall be responsible for controlling user access to the internet, as well as for ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security breaches and incidents.

7.3.6.2.3. Incoming e-mails must be treated with the utmost care to its inherent Information Security risks. The opening of e-mails with file attachments is not permitted unless such attachments have already been scanned for possible computer viruses or other malicious code.

7.3.6.3. Use of laptop computers

7.3.6.3.1. Usage of laptop computers by employees of the University of Venda is restricted to business purposes only, and users shall be aware of, and accept the terms and conditions of use, especially the responsibility for the security of information held on such devices.

7.3.6.3.2. The information stored on a laptop computer of the University of Venda shall be suitably protected at all times, in line with the protection measures prescribed in the IT Security Directive.

7.3.6.3.3. Employees shall also be responsible for implementing the appropriate security measures for the physical protection of laptop computers at all times, in line with the protection measures prescribed in the IT Security Directive.

7.3.6.4. Communication security

7.3.6.4.1. The application of appropriate security measures shall be instituted in order to protect all sensitive and confidential communication of the University of Venda in all its forms and at all times.

7.3.6.4.2. All sensitive electronic communications by employees, contractors or employees of the University of Venda must be encrypted in accordance with COMSEC standard and the Communication Security Directive of the University of Venda. Encryption devices shall only be purchased from COMSEC and will not be purchased from commercial suppliers.

7.3.6.4.3. Access to communication security equipment of the University of Venda and the handling of information transmitted and/ or received by such equipment, shall be restricted to authorized personnel only (personnel with Top Secret Clearance who successfully completed the COMSEC Course).

7.3.6.5. Technical surveillance counter measures (TSCM)

7.3.6.5.1. All offices, meeting, conference and board room venues of the University of Venda where sensitive and classified matters are discussed on a regular basis shall be identified and shall be subjected to proper and effective physical security and access control measures. Periodic electronic Technical Surveillance Counter Measure (sweeping) will be conducted by the State Security Agency (SSA) to ensure that these areas are kept sterile and secure.

7.3.6.5.2. The Security Director of the University of Venda shall ensure that areas that are utilized for discussion of a sensitive nature as well as offices or rooms that house electronic communications equipments, are physically secured in accordance with the standards laid down by the State Security Agency (SSA) in order to support the sterility of the environment after a Technical surveillance counter measures examination, before any request for a Technical surveillance counter measures examination is submitted.

7.3.6.5.3. No unauthorized electronic devices shall be allowed in any boardrooms and conference facilities where sensitive information of the University of Venda is discussed. Authorization must be obtained from the Security Manager.

7.3.7. Business Continuity Plan (BCP)

7.3.7.1. The Security Director of the University of Venda must establish a Business Continuity Plan (BCP) to provide for the continued availability of critical services, information and assets if threat materializes and to provide for appropriate steps and procedures to respond to an emergency situation to ensure the safety of employees, contractors, consultants and visitors.

7.3.7.2. The Business Continuity Plan shall be periodically tested to ensure that the management and employees of the University of Venda understand how it is to be executed.

7.3.7.3. All employees of the University of Venda shall be made aware and trained on the content of the Business Continuity Plan to ensure understanding of their own respective roles in terms thereof.

7.3.7.4. The Business Continuity Plan shall be kept up to date and re-tested periodically by the Security Manager.

1. **SPECIFIC RESPONSIBILITIES**
	1. **Head of Institution**
		1. The Principal of the University of Venda bears the overall responsibility for implementing and enforcing the security program of the University of Venda. Towards the executing of this responsibility, the Principal shall:
* Establish the post of the Security Manager and appoint a well trained and competent security official in the post;
* Establish a security committee for the institution and ensure the participation of all senior management members of all core business functions of the University of Venda in the activities of the committee;
* Approve and ensure compliance with this policy and its associated Security Directives by all it is applicable to.
	1. **Director Security**

5.2.1. The delegated security responsibility lies with the Security Manager of the University of Venda who will be responsible for the execution of the entire function and program within the University of Venda (coordination, planning, implementing, controlling, etc). Towards execution of his/her responsibilities, the Director Security shall amongst others:

* Chair the security committee of the University of Venda
* Draft the internal Security Policy and Security Plan ( containing the specific and detailed Security Directives) of the University of Venda in conjunction with the security committee;
* Review the Security Policy and Security Plan at regular intervals;
* Conduct a security TRA of the University of Venda with the assistance of the security committee;
* Advice management on the security implications of management decisions;
* Implement a security awareness program;
* Conduct internal compliance audits and inspections at the University of Venda at a regular intervals;
* Establish a good working relationship with both State Security Agency and South African Police Services and liaise with these institutions on a regular basis.
	1. **Security Committee**
		1. The Security Committee referred to in par 8.1.1. above shall consist of senior managers of the University of Venda representing all the main business units of the University of Venda.
		2. Participation in the activities of the Security Committee by the appointed representatives of business units of the University of Venda shall be compulsory.
		3. The Security Committee of the University of Venda shall be responsible for amongst others:
* Assisting the Security Manager in the executing of all security related responsibilities at the University of Venda, including completing tasks such as drafting/reviewing of the Security Policy and Plan, conducting a security Threat and Risk Assessment, conducting of security audits, drafting of a Business Continuity Plan and assisting with security awareness and training.
	1. **Line Management**

These staff members have a pivotal role in promoting security within their areas of responsibility. They are responsible for:

* + 1. Ensuring that staff have access to and are familiar with the Security Policy, paying particular attention to those issues which are relevant to the activity of their department.
		2. Ensuring that all members of staff and students in their department understand and exercise their security responsibilities and have due regard to university property in particular the security of IT equipments.
		3. Liaise with Protection Services on any security matter and attend security coordination meetings if required.
		4. Undertaking a security risk analysis of their department areas and operations, in liaison with the Protection Services and acting to remove or reduce as far as possible, any security risks.
		5. Maintaining equipment inventories.
		6. Controlling access to their departmental areas by taking responsibility for the issue of keys.
		7. Ensuring that their departmental staff returns to the department any issued keys on their last day of work.
		8. Notifying Protection Services of any risk (including the purchase of expensive equipment etc) who will then advice on any additional security or protection and investigate any crime or incident.
	1. **Staff**

(This includes all those with a contract of work, including research staff, visiting lecturers and anyone employed as a tutor, supervisor or lecturer on a temporary basis). All staff must ensure they are familiar with and follow the procedures in the Security Policy, paying particular attention to those issues which are relevant to their activities. They must also cooperate with requests from Protection Services especially with emergency or evacuation instructions and in relation to Security procedures.

* 1. **Students**

Students have a general responsibility to look after university facilities properly and to give due consideration to security issues. They must follow security procedures designed to protect the University, community and property, in particular regulations governing access to computer rooms or areas with other public use equipment. Students must cooperate with request from Protection Services, especially with emergency or evacuation instructions and in relation to security procedures.

* 1. **Visitors.**

Visitors including conference delegates and event attendees have a general responsibility to look after the University facilities whilst on campus and to give due consideration to security issues. In particular they follow must security procedures designed to protect University property. Visitors must follow instructions from Protection Services or from their host department, particularly in emergency situations.

* 1. **Common Areas**

Security risks in common or public areas of buildings are the responsibility of University as a whole but will be devolve responsibility of the Campus Director. Campus Directors are requested to draw particular risk or issues to the attention of Protection Services, so that effective solutions can be proposed in conjunction with all interested parties.

1. **AUDIENCE**

8.1. This Policy is applicable to all members of the management, employees, consultant, contractors and any other service provider of the University of Venda. It is further applicable to all visitors and members of the public visiting premises of or may officially interact with the University of Venda.

1. **ENFORCEMENT**
	1. The Principal of the University of Venda and the appointed Director of Security are accountable for the enforcement of this policy.
	2. All employees of the University of Venda are requested to fully comply with this policy and it’s associated Security Directives as contained in the Security Plan. Non-compliance with any prescripts shall be addressed in terms of the Disciplinary Code/Regulations of the University of Venda.
	3. Prescripts to ensure compliance to this policy and the Security Directives by all consultants, contracts signed with such individuals/institutions/companies.

The consequences of any transgression/deviation or non-compliance shall be clearly stipulated in said contracts and shall be strictly enforced. Such consequences may include the payment of prescribed penalties or termination of the contract, depending on the nature of any non-compliance.

1. **EXCEPTIONS**
	1. Deviations from this policy and its associated Security Directives will only be permitted in the following circumstances:
* When security must be breached in order to save or protect the lives of people.
* During unavoidable emergency circumstances e.g. natural disasters;
* On written permission of the Principal of the University of Venda (reasons for allowing no-compliance to one or more aspects of the policy and directives shall be clearly stated in such permission; no blanket non-compliance shall be allowed under any circumstances).
1. **OTHER CONSIDERATIONS**
	1. The following shall be taken into consideration when implementing this policy:
* Occupational Health and Safety issues in the University.
* Disaster management at the University.
* Disabled persons shall not be inconvenienced by physical security measures and must be catered for in such a manner that they have access without compromising security or the integrity of this policy.
* Environmental issues as prescribed and regulated in relevant legislation (e.g. when implementing physical security measures that may impact on the environment).
1. **COMMUNICATING THE POLICY**
	1. The Security Director of the University of Venda shall ensure that the content of this policy (or applicable aspects thereof) is communicated to all employees, consultants, contractors, service providers, clients, visitors, members of the public that may officially interact with the University of Venda. The Security Manager will further ensure that all security policy and directives prescriptions are enforced and complied with.
	2. The Security Director must ensure that a comprehensive security awareness program is developed and implemented within the University of Venda to facilitate the above said communication. Communication of the policy by means of this program shall be conducted as follows:
* Awareness workshops and briefings to be attended by all employees;
* Distribution of memos and circulars to all employees;
* Access to the policy and applicable directives on the intranet of the University of Venda.
1. **REVIEW AND UPDATE PROCESS**
* The Security Director, assisted by the Security Committee of the University of Venda must ensure that this policy and its associated Security Directives is reviewed and updated on an annual basis. Amendments shall be made to the policy and the directives as the need arise.
1. **IMPLEMENTATION**
* The Director Security of the University of Venda must manage the implementation process of this policy and its associated Security Directives (contained in the Security Plan) by means of an action plan (also to be included in the security plan of the University of Venda).
* Implementation of the policy and its associated Security Directives is the responsibility of each and every individual this policy is applicable too.
1. **MONITORING OF COMPLIANCE**
* The Director Security, with the assistance of the security component and security committee of the University of Venda must ensure compliance with this policy and its associated Security Directives by means of conducting internal security audits and inspections on a frequent basis.
* The findings of said audits and inspections shall be reported to the Principal of the University of Venda forthwith after the completion thereof.
1. **DISCIPLINARY ACTION**
* Non-compliance with this policy and its associated Security Directives shall resulting disciplinary action which may include, but are not limited to:
* Re-training
* Verbal and written warning
* Termination of contracts in the case of contractors or consultants delivering a service to the University of Venda
* Dismissal
* Suspension
* Loss of University of Venda information and assets resources access privileges
* Any disciplinary action taken in terms of non compliance with this policy and its associated directives will be in accordance with the disciplinary code/directive of the University of Venda.
1. **GLOSSARY**
* Accreditation means the official authorisation by management for the operation of an Information Technology System, and acceptance by that management of the associated residual risk. Accreditation is based on the certification process as well as other management considerations;
* Assets mean material and immaterial property of an institution. Assets include but are not limited to information in all forms and stored on any media, networks or systems, or material, real property, financial resources, employee trust, public confidence and international reputation
* Availability means the condition of being usable on demand to support operations, programmes and services;
* Business continuity plan includes the development of plans, measures, procedures and arrangements to ensure minimal or no interruption of the availability of critical services and assets;
* Candidate means an applicant, an employee, a contract employee or a person acting on behalf of a contract appointee or independent contractor;
* Certification means the issuing of a certificate certifying that a comprehensive evaluation of the technical and non-technical security features of an information and communication technology system and its related safeguards has been undertaken and that it was established that its design and implementation meets a specific set of security requirements;
* COMSEC means the organ of state known as Electronic Communications Security (pty)Ltd, which was established in terms of section 2 of the Electronic Communications Security Act,2002(Act no. 68 of 2002) and, until such time as COMSEC becomes operational, the South African Communication Security Agency;
* Critical services means a service identified by an institution as a critical service through a Threat and Risk Assessment and the compromise of which will endanger the effective functioning of the institution;
* Document means
* Any note or writing, whether produced by hand or by printing, typewriting or any other similar process, in either tangible or electronic format;
* Any copy, plan, picture , sketch or photographic or other representation of any place or article;
* Any disk, tape, card, perforated roll or other device in or on which sound or any signal has been recorded for reproduction;
* Information security include but is not limited to,-
* Document security;
* Physical security measures for the protection of information;
* Information and communication technology security;
* Personnel security;
* Business continuity plan;
* Contingency planning;
* Security screening;
* Technical surveillance counter measures;
* Dealing with information security breaches;
* Security investigations; and
* Administration and organization of the security function at organs of state;
* National intelligence structures means the National Intelligence Structures as defined in section 1 of the National Strategic Intelligence Act, Act 34 of 1994;
* Reliability checks means an investigation into the criminal record, credit record and past performance of an individual or private organ of state to determine his , her or its reliability;
* Risk means the likelihood of a threat materialising by exploitation of a vulnerability;
* Screening investigator means a staff member of a National intelligence structure designed by the head of the relevant National Intelligence Structure to conduct security clearance investigations;
* Security breach means the negligent or intentional transgression of or failure to comply with security measures;
* Security clearance means a certificate issued to a candidate after the successful completion of a security screening investigation, specifying the level of classified information to which the candidate may have access subject to the need to know;
* Site access clearance means clearance required for access to installations critical to the national interest;
* Technical surveillance countermeasures means the process involved in the detection, localisation, identification and neutralisation of technical surveillance of an individual, an organ of state, facility or vehicle;
* Technical / electronic surveillance means the interception or monitoring of sensitive or proprietary information or activities (also referred to as bugging);
* Threat means any potential event or act, deliberate or accidental, that could cause injury to persons, compromise the integrity of information or could cause the loss or damage of assets;
* Threat and Risk assessment means within the context of security management, the process through which it is determined when to avoid, reduce and accept risk, as well as how to diminish the potential impact of a threatening event;
* Vulnerability means a deficiency related to security that could permit a threat to materialise.

**DEVELOPED BY: MULAUDZI RATSHILUMELA**

**HEAD OF SECURITY**

**RECOMMENDED BY: ADV AE MUSHAVHANAMADI**

**HEAD: CAMPUS CONTROL**

**APPROVED BY:**