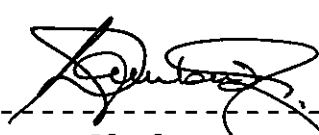


Policy library ID  
ICT: 06



# IT Security Policy

<b>Sponsor division</b>	Operations and ICT Services
<b>Responsible Department</b>	ICT Services
<b>Related WSU policies</b>	
<b>Policy name</b>	<b>Policy Name</b>
Computing Passwords Policy	Acceptable Use Policy
<b>Change History</b>	
<b>Approval authority</b>	<b>Council</b>
<b>Approval Date</b>	<b>24 November 2017</b>
<b>Latest revision date</b>	<b>November 2020</b>
<b>Effective date</b>	<b>Immediately</b>
<b>Number of pages</b>	<b>14</b>
 ----- <b>Chairperson of Council</b>	

## Contents

<b>1. Preamble .....</b>	<b>3</b>
<b>2. Purpose .....</b>	<b>3</b>
<b>3. Scope .....</b>	<b>3 - 4</b>
<b>4. Definitions .....</b>	<b>4 - 5</b>
<b>5. Policy Implementation .....</b>	<b>5 - 13</b>
<b>6. Policy Review .....</b>	<b>13</b>
<b>7. Related Policies .....</b>	<b>13</b>

## **1. PREAMBLE**

Walter Sisulu University (WSU) recognises the role of information security in ensuring that users have access to the information they require in order to carry out their work. Computer and information systems underpin all the University's activities, and are essential to its research, teaching, community engagement and administrative functions.

Any reduction in the confidentiality, integrity or availability of information could prevent the university from functioning efficiently and effectively. Furthermore, the loss or unauthorised disclosure of information has the potential to damage the University's reputation and cause financial loss.

To mitigate these risks, information security must be an integral part of information management. The University is committed to protecting the security of its information and information systems in order to ensure that:

- a. The integrity of information is maintained, so that it is accurate and up to date.
- b. Information is always available to those who need it and there is no disruption to the business of the University.
- c. Confidentiality is not breached, so that information is accessed only by those authorised to do so.
- d. The University meets its legal requirements, including those applicable to personal data under the Data Protection Act.
- e. The reputation of the University is safeguarded.

The University aims to frequently perform information security risk assessments for all information systems on a regular basis in order to identify key information risks and determine the controls required to keep those risks within acceptable limits.

## **2. PURPOSE**

The purpose of this policy is to provide a framework for the management of information security at WSU.

## **3. SCOPE**

This policy applies to:

- a. All those with access to University information systems, including staff, students, visitors and service providers
- b. Any systems attached to the University computer or telephone networks and any systems supplied by the University.
- c. All information processed by the University pursuant to its operational activities, any communications sent to or from the University and any University information held on systems external to the University's network.

- d. All external parties that provide services to the University in respect of information processing facilities and business activities.
- e. Principal information assets including the physical locations from which the University operates.

#### **4. DEFINITIONS**

Any definitions listed below apply to this document only with no implied or intended institution-wide use.

**"Confidentiality"** - limit access or place restrictions on certain types of information.

**"Integrity"** – the absence of alteration between two instances or between two updates of a data record.

**"Availability"** - the degree to which a system, subsystem or equipment is in a specified operable and committable state.

**"Security Alerts"** - A sound or message that indicates some predefined measures that are taken to protect a resource.

**"Technical Documentation"** - describes the handling, functionality and architecture of a product or a product under development or use.

**"Third Party Services"** – provisions offered by external organizations.

**"Information Technology Steering Committee (ITSC)"** - a Sub-Committee of the Institutional Management Committee (IMC) with the strategic responsibility of prioritising IT investment programmes in line with university strategic plan, track status of projects and resolve resource conflicts as well as monitor service levels and service improvements.

**"Institutional Management Committee (IMC)"** - highest leadership organ of the university that reports to the Council.

**"Encryption"** - the conversion of electronic data to a format, which cannot be easily understood by anyone except authorized parties.

**"Virtual Private Network (VPN)"** - a network that is constructed by using public network, usually the Internet to connect to a private network, such as a company's internal network .

**"Chain Letters"** - a letter sent to a number of people, each of whom is asked to make and mail copies to other people who are to do likewise, often used as a means of spreading a message or raising money.

**"Domain Name System (DNS)"** - a system for naming computers and network services that is organized into a hierarchy of domains. DNS naming is used in

Transport Communication Protocol/Internet Protocol (TCP/IP) networks, such as the Internet, to locate computers and services through user-friendly names.

**“Dynamic Host Configuration Protocol (DHCP)”** - a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

**“Sanitize”** - make a resource more palatable by removing elements that are likely to be unacceptable or controversial.

**“Digital Signature”** - a technique used to validate the authenticity and integrity of a message, software or digital document and is intended to solve the problem of tampering and impersonation in digital communications.

## **5. POLICY IMPLEMENTATION**

### **5.1. Security Roles and Responsibilities**

Information technology security is the responsibility of all staff and students. Every person handling information or using university information resources is expected to observe this policy. Information and Communication Technology (ICT) Services Department will provide assistance to all members of the university community to facilitate compliance through the publication of information technology security alerts, guidelines, technical documentation and ongoing awareness program.

Individual end users control access to their computing devices and the files and applications installed in them. Therefore, the user is responsible for determining who has access to locally stored data and applications and for managing the appropriate levels of access.

### **5.2. Standards**

WSU’s technology environment is a shared and limited resources that could be prone to malicious and unintended abuse. Computing systems and other specialized devices have the potential to introduce security risks especially when connected to the network. To mitigate risk, standards for managing and securing applications, workstations, servers, network devices and third-party services have been developed.

As new equipment or applications are introduced into the environment, a risk assessment should be conducted to ensure compliance with set standards. ICT Services staff and university’s internal and external auditors will periodically conduct compliance reviews and test vulnerabilities. This will ensure systems and applications are updated as new vulnerabilities emerge and threats revealed

## **5.3. Requirements**

### **5.3.1 General**

#### **5.3.1.1 Network User Names and Passwords**

Logical access controls can prevent or discourage unauthorized access to information resources and help ensure individual accountability. Therefore, individual users must be identified and granted appropriate levels of access to network devices by means of a unique User Name coupled by a password. A unique User Name is required to provide for individual accountability. For this reason, a generic or group identities are not permitted.

Default manufacturer passwords must be changed. Replacement passwords must be composed in accordance with the Computing Passwords Policy which adopts the following naming convention:

- a. Passwords must be at least eight (8) characters in length and be composed of both letters and numbers
- b. Passwords may not be repeated within the past year
- c. Passwords should be changed frequently, but are required to change every six months

#### **5.3.1.2 Secure Verification of User Name and Password**

Under certain conditions, it is possible to eavesdrop on network traffic. For this reason, User Name and password authentication procedures must use an encryption mechanism. This implies that encrypted versions of email, file transfer, server, desktop administration and other network access programs may be used.

#### **5.3.1.3 Third-Party Services**

When a third-party is used to provide services or store data, security requirements should be considered and made part of any contractual agreements. Such vendor agreements must include appropriate safeguards for the security of the university's information resources and audit rights. Vendors may only have access to the minimum necessary information to perform the tasks for which they have been retained. Vendor access must be uniquely identifiable and major activities should be logged. These activities include, personnel changes, password changes, milestones reached and deliverables.

Upon departure of a vendor employee, the vendor must be required to return or destroy all sensitive information and surrender WSU identification badges, access cards, equipment and supplies.

## **5.3.2 Hardware**

### **5.3.2.1 Device Registration**

Each device must be registered upon first use and re-registered at the frequency in effect for the type of user. In order to register a device, the user must provide the unique network media access control (MAC) hardware identifier assigned to the device by its manufacturer and a valid WSU network User Name.

### **5.3.2.2 Assignment of Network Identifiers**

In order to ensure reliable network operation, all devices must be configured to accept the assigned Internet Protocol (IP) numeric address, WSU generated identifying name and other network parameters which are automatically assigned each time a network connection is established. The use of permanent network identifiers is restricted to ICT Services managed or approved devices.

### **5.3.2.3 Equipment Sanitization on Disposal**

Sensitive university academic and administrative information is likely to be present on storage media associated with obsolete or surplus equipment intended for disposal. University-owned IT equipment must therefore be disposed of according to the Equipment Disposal Policy and fully sanitized in a way that secures sensitive data and licensed software.

### **5.3.2.4 Server Registration**

If a network device provides services to multiple users, there are additional registration requirements since allowing outside systems to initiate connections to a university system increases threats from the Internet. Publicly accessible systems must therefore be registered with ICT Services. Registration information will include name and contact information for the person who is responsible for administering it and verification that security configurations are in place. The administrator must describe any confidential data stored on the system.

### **5.3.2.5 Departments and Administrative Units**

Departments and administrative units are responsible for ensuring the security and safety of publicly accessible systems in their environments.

## **5.3.3 Software**

### **5.3.3.1 Anti-Virus Software**

Computers infected with viruses or malicious code can jeopardize information technology security by contaminating, damaging and destroying data. Therefore

anti-virus software must be installed and frequently updated with the most current list of virus definitions. The university has licensed anti-virus software for use by the WSU community.

#### **5.3.3.2 Firewall Software**

All end user devices must use firewall software configured according to WSU guidelines.

#### **5.3.3.3 Licensed Software**

Software installed on any WSU computer system must be legally licensed. Audits may be conducted at any time to ensure this objective is met. Departmental and administrative unit heads are responsible for ensuring that no software license usage in their sections exceeds purchased levels and arranging for additional licensed copies when needed to support instructional and administrative activities.

The use of open source and freeware software is permitted subject to approval by ICT Services Department.

#### **5.3.3.4 Software Patch Updates**

All currently available security patches for operating systems and application software must be installed. Software for which security patches are not routinely made available should not be used on the WSU network.

#### **5.3.3.5 End Point "Health Check"**

All computers connected to WSU network are required to undergo an automated evaluation to determine if certain software settings and applications are correctly installed and operational. The result of this evaluation may require the user to install new software or reconfigure existing software before unlimited network access is granted.

The university will not access or modify software or information stored on personally owned equipment without permission of the owner. However, access to the WSU network may be denied or limited unless this policy is complied with fully.

#### **5.3.3.6 Secure Data Transmission**

When employees are working at an off-campus location and remotely connecting to systems on the WSU network, an encrypted communication channel must be used in order to protect the confidentiality of User Names, passwords and university records containing personal, confidential or legally protected information. This is also necessary when using the on-campus wireless network.



A general purpose encrypted communication link can be accomplished through use of "virtual private network (VPN)" technology. By accessing WSU network via a special web interface, the stipulated security requirements will be met. When using university VPN technology with personal equipment, users must understand that their machines are acting as extensions of WSU network and are therefore subject to the same requirements that apply to WSU owned equipment.

### **5.3.3.7 Digital Signatures**

A digital signature is an electronic equivalent of a handwritten signature or stamped seal, but offering far more inherent security. It is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer.

Electronic communication involving the transfer of confidential documents or data must include the use of digital signatures.

### **5.3.3.8 Secure Data Storage**

Sensitive personal information must be stored within university systems using approved method of encryption to help secure the data in the event of unauthorized access. This requirement is particularly important when information is stored on portable devices.

## **5.4. Prohibited Practices**

### **5.4.1 General Activities**

Users must not purposely engage in activities that may harass, threaten or abuse others. In addition, activities that may degrade the performance of information resources and deprive authorized users access to a technology resource are prohibited. Any attempt to circumvent WSU security measures is not allowed.

Users must not attempt to access data or programs for which they have no authorization and may not share accounts, passwords, security tokens or similar information or devices used for identification and authorization purposes.

Users must not take any action that violates the university's code of conduct, academic integrity, information technology security policy or other applicable policy of law. In the event of a conflict between policies, the more restrictive policy shall govern.

#### **5.4.2 Commercial Use**

WSU information technology resources may not be used for solicitations, commercial purposes or any business activities for individuals, groups or organizations without prior permission from the Vice Chancellor.

#### **5.4.3 Copyright and Illegal Software and Materials**

Users are prohibited from making or using illegal copies of copyrighted materials or software. This includes illegal downloads from the Internet. No illegal copies of such materials may be stored on university systems or transmitted over the university network. Users may not copy software applications from one PC to another unless legally permitted.

#### **5.4.4 Email**

The following activities are prohibited because they impede the functioning of electronic mail systems and may expose sensitive data to unauthorized access:

- a. Sending or forwarding chain letters
- b. Sending unsolicited messages to large groups, except when necessary to fulfil the academic and administrative mission of the university
- c. Sending of excessively large (for example 30 Mbytes) or numerous (for example over 500) messages except when coordinated in advance by ICT Services
- d. Intentionally sending or forwarding e-mail containing computer viruses
- e. Sending, forwarding or receiving confidential or sensitive academic or administrative information through non-WSU e-mail accounts. That is e-mail provided by Internet service providers such as Yahoo and Google. Confidential WSU information must not be stored or transmitted through public facilities.

#### **5.4.5 Network Monitoring**

Users may not conduct network scans searching for other connected devices or conduct any form of network monitoring that will intercept data not intended for the user's computer. Users must not download, install or run programs designed to reveal or exploit weaknesses in system security such as password discovery programs, packet sniffers or port scanners.

#### **5.4.6 Server and Network Operations**

Unless specific authorization is received from ICT Services, individual users or departments must not operate DHCP, DNS, proxy, email, remote access or connection sharing servers. Users may not implement individual or departmental servers for anything other than academic purposes. Examples of prohibited servers could include music, video sharing and gaming servers. External DNS providers may

not be caused to advertise services at WSU. Users or departments must not install network components such as switches, routers or wireless access points. Tampering with any network cabling is prohibited. ICT Services approved hub devices are permitted.

#### **5.4.7 Wireless Communication**

Installation, maintenance and operation of wired and wireless networks serving WSU community are the sole responsibility of ICT Services. Individual or departments may not independently deploy wireless networking products without the involvement of ICT Services.

### **5.5. Enforcement**

Violations of this policy must be reported to ICT Services who will investigate the incident and take appropriate remedial actions. Remedial actions could include the following:

- a. Temporary or permanent withdrawal of access privileges
- b. Prescribed university sanctions including dismissal
- c. Remedial education
- d. Monetary reimbursement to the university
- e. Prosecution under applicable civil or criminal laws

#### **5.5.1 Monitoring Compliance**

In order to ensure compliance with this policy, ICT Services may:

- a. Monitor network traffic for the detection of unauthorized activity and intrusion attempts
- b. View or scan any file or software stored on university systems or transmitted over university networks.
- c. Carry out and review the results of automated network-based security scans of systems and devices on the university network in order to detect known vulnerabilities or compromised hosts.
- d. Report recurring vulnerabilities over multiple scans to the respective departmental or unit head
- e. Take steps to disable network access to affected systems or devices if identified security vulnerabilities deemed to be a significant risk to others have been reported
- f. Act to contain the problem by isolating systems or devices from the network
- g. Coordinate investigations into any alleged computer or network security incidents
- h. Cooperate in the identification and prosecution of activities that violate this policy

Violations, complaints or questions regarding this policy should be directed to: [iss@wsu.ac.za](mailto:iss@wsu.ac.za).

## **5.6. Access to University Records**

The university provides limited access to academic and administrative data to those whose educational and administrative responsibilities require it to perform their job function. Multiple levels of access exist which are generally determined by the nature of the position held. This practise helps to ensure that data access restrictions are consistent and based on legal, ethical and practical considerations. The university expects all custodians of its academic and administrative records to access and utilize this information in a manner consistent with the university's need for security, integrity and confidentiality. Each university functional unit must develop and maintain clear and consistent procedures for access to data within its area of responsibility and review access levels and procedures regularly.

### **5.6.1 Access Rights and Responsibilities**

Access rights for certain applications are assigned on application by the user and recommendation from data owners. Departmental managers must ensure that their representatives maintain only those access privileges required to perform their official job functions. Users may only access, change or delete data as required in fulfilment of assigned university duties. The following is a list of some prohibited activities:

- a. Do not change data about yourself or others for reasons other than usual administrative purposes
- b. Do not use information to support actions by which individuals might profit (e.g. change in salary or student marks)
- c. Do not disclose information about individuals without prior supervisor authorization
- d. Do not engage in any type of unauthorized data analyses (e.g. tracing a pattern of salary increases or determining the source and destination of telephone calls)
- e. Do not circumvent the nature or level of data access given to others
- f. Do not facilitate another's illegal access to WSU administrative systems by sharing your passwords
- g. Do not release institutional data to internal, external organizations or government agencies without prior approval from your supervisor

### **5.6.2 Privacy**

All files created or maintained on university owned computer resources are subject to WSU privacy policies. While access to files is limited to those intended to have it, authorized university officials can examine the contents of all files and operational logs. The university reserves the right to view or scan any file or software stored on its systems or transmitted over its networks. This will be done periodically to verify that software and hardware are working correctly, preserve data for backup

purposes, to look for disruptive forms of data or software, to audit the use of university resources and to ensure compliance with the law and university policies.

Personal computing devices that connect to the university network are subject to the same requirements that apply to WSU issued equipment.

All files are further subject to external review and possible public release resulting from a search warrant or subpoena issued and served pursuant to law.

### **5.7. Data Backup and Recovery**

Production servers and computers offering shared network resources are backed up regularly to provide protection against hardware failures and other disasters. Individual computers are not backed up by ICT Services. It is strongly recommended that users make individual backups of critical data. This may be done by copying important information to the user's network storage drive, which is backed up by ICT Services on a regular basis.

### **5.8. Security Awareness and Training**

It is essential that all aspects of information security, including confidentiality, privacy and procedures relating to system access be incorporated into formal student and staff orientation procedures and conveyed to existing university community members on a regular basis.

ICT Services holds semi-annual meetings with departmental technical partners at which current and pending security issues and new potential risks are discussed and mitigation strategies shared. ICT Services also hosts security web pages containing resources on information and system security.

Managers should review at least annually or upon job description change the duties of personnel under their supervision to determine if the position is one of special trust. Personnel whose duties bring them into contact with confidential or sensitive information should be required to provide written assurance of their intention to comply with the university security policies and attend an awareness and training program at least annually and receive periodic security briefings as necessary.

## **6. POLICY REVIEW**

This policy should be reviewed every three years, or as changes in legislation or technology dictate. Changes to the policy should be referred to the ITSC, who will refer any substantive changes to the IMC and Council.

This policy refers to a number of related guidelines and policies. Unless otherwise specified in a specific document, revisions to those documents may happen more

frequently, and major changes need only be approved by the ITSC. However, the ITSC, at its discretion, may refer these to IMC or Council.

## **7. RELATED POLICIES**

- a. Computing Passwords Policy
- b. Acceptable Use Policy