University of Fort Hare
Information Security Policy

University of Fort Hare
Together in Excellence

Policy number	**ICT004**			
Policy Version Number	Version 1.0			
Policy originator / owner	Information, Communications and Technology			
	Date	**Minute ref**	**Name**	**Signature**
Approved by EMT				
Approved by Senate				
Approved by JBF				
Approved by Council				
Next review date	January 2018			

Information Security Policy

1. General

Policy statement and Scope

University of Fort Hare has a vast store of information, ranging from administrative such as salaries, accounts and examination results to proprietary information such as information produced by the students and lecturers. As with any education institution, the sharing of information, gathering of information and security policy needs to form a balance protecting its core resource, information, and enhancing learning through the sharing of information.

The security of information is paramount to the ongoing confidentiality, integrity and availability of University of Fort Hare information systems and for deriving the maximum return on the investment in Information Technology possible. University of Fort Hare is continually upgrading and investing in its Information Technology Infrastructure.

This policy is intended for all users of University of Fort Hare ICT infrastructure and standalone systems. The following principles, standards and procedures have been established to formalize the information security process at University of Fort Hare.

All information traveling over University of Fort Hare computer networks that has not been specifically identified as the property of other parties will be treated as though it is a University of Fort Hare.

Objective

The purpose of this policy is to ensure that due care is exercised in protecting University of Fort Hare information systems and data. Due care is defined as the cost-effective protection of information at a level appropriate to its value. The value of the information can be quantified as the risk to University of Fort Hare if the information was lost or compromised. As such, the objectives of this policy are to :

Provide direction as to what UFH wants to achieve regarding information Security.
Promote awareness amongst all, staff (academic and operational), students, Contractors and consultants of the value of information and the risks involved In working with or handling information.
Provide the necessary protection of information, thereby ensuring its confidentiality, integrity and availability.

Introduction

Information security has three dimensions: confidentiality (the sensitivity of the information to unauthorized disclosure); integrity (the accuracy of information and the authenticity of transactions); and availability (the needs to have access to the information on demand0). This policy will address all three of the dimensions.
This UFH Information Security Policy applies to:

All UFH staff and students, including temporary workers, and independent contractors working for UFH.
All electronic information, including

- Data processed and stored on line, e.g. information on the network, or personal hard drives
- Backed up data
- Archived data, or other off line storage, such as palm tops
- Audit logs
- Data stored on compact discs (CDs) or floppy disks
- E-mail
- Information printed from UFH information systems

Information in all stages of its life cycle, from creation through entry, processing, communication, dissemination and storage, to disposal.

Compliance

It is necessary to enforce this information security policy in order to protect UFH legal rights. Any staff member, student or contractor who does not comply with the spirit and intent of this policy and its supporting standards will be subject to appropriate disciplinary action. This may include, revoking of access privileges, termination of agreements or contracts, or dismissal. Security breaches must be reported to the head of Information and Communication Technology Services (ICT) department as soon as the breach is suspected or becomes known.

Definitions

The following definitions will be used throughout this policy document:

- The **UFH Information and Communication Technology (ICT) infrastructure** is defined as the network (LAN and WAN) and peripherals controlled and maintained by UFH Information and Communication Technology Services(ICTS) department.

- A **standalone system** is any computer not connected to UFH ICT infrastructure. A single point of integration between the standalone system and UFH ICT infrastructure may exist.

- A **computer room** is defined as any person who is authorized to use UFH ICT infrastructure and standalone systems.

- An **Information Owner** is responsible for the overall administration and ownership of application system (e.g. salaries, exam results, etc

- **On – Site** is defined as any area of work within the general operational area of UFH. This includes the remote campuses.

- **Off- site** is defined as any residential home or property, and any location outside the general operational area.
- **Business data** is defined as any data required for the completion of daily tasks and duties. This includes Microsoft Excel spreadsheets and Microsoft Word Documents.

- **Sanitised data** is production information that no longer contains specific details that might be restricted or confidential. This data is typically used for testing and training purposes.

Roles and Responsibilities

Information security is achieved when information is protected from unauthorized disclosure, unauthorized manipulation, and loss at all stages of its life- cycle. Each staff member and student holds one or more or the following roles when dealing with information.

ROLES	RESPONSIBILITIES
Management	The responsibilities of UFH management include: Accepting accountability for the information assets Under their control Having a fiduciary duty to protect its information Assets from a variety of treats such as error, fraud, Embezzlement, sabotage, terrorism, extortion, Industrial espionage, privacy violation, service Interruption, and natural disaster. Providing the appropriate resource, including both Personnel and financial, for information asset Protection. Responding to identified exposures and vulnerabilities Supporting the investigation and resolution of

	Information – related losses and incidents Ensuring that the UFH security agreement is signed by All staff, students and independent contractors.
Information owners Data management	The owner of information is usually the person Responsible for the creation of the information or is the primary user of the information or is the primary user of the information . Owners' responsibilities includes Classifying the information in terms of this policy Authorizing access to the information Assigning an information custodian Specifying and communicating the security Requirements Implementing the security guidelines and standards contained in this policy handling day-to-day security lapses and reporting security breaches to the head of Information Technology.
Information users	the users is anyone who is authorized to read, enter, update or Delete the information. The user must: Ensure complete awareness of the content of this security Policy and its implication Only access those information system and data to which they Are specifically authorized Use the information only for the purpose intended by the owner Comply with all security measures established Report security breaches to the head of information Technology Not disclose confidential information to anyone without the Permission of the owner Sign and comply with UFH security agreement
Information custodian (Data owner)	the custodian is the person responsible for processing Or storing the information. The custodian is responsible for Administering the controls specified by the owner Reporting any security breaches to the head of information Technology
System Administrator	The system administrator is the person responsible for ensuring that the infrastructure used to store and process the information is maintained appropriately. The system administrator is responsible for:

	Ensuring that appropriate virus protection and detection measures and controls are in place throughout UFH Monitoring network activity for potential security breaches
Contractors	All contractors with access to electronic information should: Ensure complete awareness of the contents of this security policy and its implications. Only access those information system and data specifically authorized Regard all UFH information collected or accessed during their interaction with UFH as confidential and, as such, may not use, disclose, transfer or amend any information gathered during their stay without the explicit consent of the information owners. Sign and comply with the UFH security agreement
Head of Information and Communication Technology Services	The role of the head of ICTS is to: co-ordinate information security within UFH develop and maintain this information security policy and supporting standards Ensure that staff, students and contractors to UFH are properly educated and aware of this information security policy and its implications on an ongoing basis Provide support in planning, implementing and administering information security Investigate security problems / breaches

Data Classification

The classification of information is a key element in the protection of information against unauthorized disclosure. Unauthorized disclosure occurs when sensitive information finds its way into the hand of staff, student or others that should not have access to this information.

Thus, the purpose of an information classification system is to:

Promote awareness amongst all UFH management, students and staff of the need to protect information against unauthorized disclosure.

Provide a framework for establishing the level of protection required to ensure that information is adequately protected when it is being processed or handled.

Data is classified according to the following classes:

Information Class	Description
Confidential	Sensitive information disclosed only to those with an identified need to know the information. The information is normally defined in terms of group rather than by individual names. This also refers to any sensitive information provided to UFH by external organizations
Internal	Information that is not sensitive but is not intended for release to the general public. When directed by UFH management, some internal information may be subject to limited release to specific external entities . Generally, internal information should be available to all UFH Staff, e.g. Corporate Policy document.
Copyright/ patent	Information that is the property of UFH and should not be copied by external parties, but is intended for release to the general public and external parties, e.g. student papers and projects
Public	Information, such as student projects, that is specifically intended for release to the general public.

2. User Identification and Authentication

Objective

Passwords are the primary means of validating a user's authority to access UFH ICT infrastructure. It is therefore imperative to have efficient and effective policies in place regarding user password management and use. These policies will enable UFH to minimize unauthorized access to its ICT infrastructure and to establish accountability of users' actions.

Principles

1. Every user and third party requiring access to the UFH ICT infrastructure and standalone systems must have a unique user ID and a personal secret password. This user ID and password will be required to establish positive identification and authentication.

2. User are accountable for all activities performed with their personal user Ids may not be used by anyone other than the individuals to whom they have been issued.

3. All users are to comply with, and sign acceptance of, the UFH Policy. Non- compliance will result in disciplinary action, which is dependent on the nature and severity of the transgression.
4. All computers that connect to UFH ICT infrastructure must make use of proper password access controls that prohibit access to resources without proper authentication procedures.

5. Every authentication process for computers connected to the University of fort hare ICT infrastructure must include a notice warning against unauthorized use and the consequences thereof.

Standards

2.3.1 ***University of fort hare password Standard***

i. Password should be a minimum of six characters in length

ii. Password should include both alphabetic and numeric characters.

iii. The use of common names and surnames, dates of birth, spouses' names or variation thereof must be avoided.

iv. Users must not construct password using a basic sequence of characters that is then partially changed based on the date or some other predictable factor (such as CJan, then CFeb)

v. A minimum password history of six passwords must be implemented. A user may not use the same password they have used previously.

vi. Password should be changed at least 45 days for general users (e.g. academic staff and students)

vii. Password should be changed at least every 30 days for privileged users (e.g. salaries administrators, network administrators)

Procedures

2.4.1 User Password Management

Responsibility: Information Custodian

i. Password are not to be written down, divulged or shared, as users will be held accountable for all actions performed on their user ID.

ii. Users will be issued with a temporary password that they must change after their first logon. This password must be communicated to the user in a secure manner and the use of email or third parties for this purpose should be avoided.

iii. If a workstation is to be left unattended for any prolonged period (more than ten minutes), users must either lock the workstation or logout of the system. Screensavers should password protected and be set to activate after standing idle for two minutes.

iv. No workstation must make use of password list (PWL) files to cache passwords. Password caching allows an unauthorized person to retrieve these password out of cache and thereby gain access to the system.

2.4.2 Password Use

i. Internal user Ids and password must not be used when subscribing to external or third party system. **Responsibility: All**

ii. Regardless of the circumstances, password must never be shared or revealed to anyone else besides the authorized user: **Responsibility: All**

iii. Account lockout should be set by the system Administrator to occur after three incorrect logon attempts. **Responsibility: System Administrator**

iv. If an account is locked out, the user should contact the ICTS help Desk who will arrange for the unlocking of the account. **Responsibility: User**

v. Passwords should be tested on a regular basic. Any users that are found to be using password in contravention of the above criteria may face disciplinary action up to and including dismissal. **Responsibility: Information Custodian**

2.4.3 Changing your password

i. Passwords must be immediately changed if their confidentiality is suspected of being compromised. **Responsibility: All**
ii. System Administrators are responsible for implementing the password policy, while users are responsible for complying with the policy requirements. **Responsibility: System Administrator**
iii. Users must not choose passwords that are identical ore substantially similar to password they have previously used. **Responsibility: User**

3 Safeguarding of information Assets and Resources

3.1 Objectives

In order to safeguard fort hare information assets and resources effectively, adequate Logical and Physical access controls are necessary for their protection from loss, misuse, disclosure or modification.

3.2 Principles

3.2.1 All IS assets and resources are the property of Fort Hare

3.2.2 Cost-effective safeguards or controls need to be implemented to adequately protect IS Assets and resources from loss, misuse, disclosure or modification.

3.2.3 The level of security afforded to IS assets and resources is determined by their value, sensitivity and criticality of Fort Hare.

3.2.4 Access to the Fort Hare ICT infrastructure and standalone systems is not open and is granted to improved users on the basis of positive identification and authority.

3.2.5 Each data type (Financial, Examination Results, etc) will have a designated owner, who will be responsible for the management of that data. The System Owner will determine users' type and level of access to data. The boundaries of data ownership will be agreed upon between the Information Owners. Custodians and at the Data Manager's forum.

3.2.6 All administrator equivalent user Ids and passwords are to be known only to the individuals responsible for the administration of the Fort Hare ICT infrastructure, applications and databases. These are to be written down and sealed in an envelope, which is to be locked in the safe of the chief Director: Finance. This information is to be accessed in emergencies only i.e. when the Database Administrator, System Owner or System Administrator is unavailable. The user Ids and password are to be changed immediately thereafter.

3.2.7 Application access is to be granted by the Head of Department owning that application, on the authority of the Information Owner.

3.2.8 The Personal and Registration Departments are to provide the ICTS Department with up-to-date and relevant staff and student details to ensure that the appropriate security controls are implemented in the light of this information. In particular, students or staff that have left the employ or registration of fort hare should have all access rights and privileges revoked.

3.2.9 Heads of Department are responsible for all responsible for all information assets and resources in their department. Fort Hare ICT infrastructure is owned by the ICTS Department.

3.3 Physical Security – Procedures

Security of Computer Rooms

3.3.1 All critical system must be housed in a computer room. **Responsibility: Facilities Manager**

3.3.2 The location and design of a computer room must take into account the Possibility of fire, flooding, and other associated damage risks. **Responsibility: Facilities Manager**

Environmental Security

3.3.3 The IS Department must provide and maintain fire detection/suppression, air Conditioning, and other computing environment protection system necessary to assure continued service for critical computer system. **Responsibility: Facilities Manager**

3.3.4 All IS equipment hosting critical systems must be protected from power Failures or other electrical anomalies. An uninterruptible power supply (UPS) must be used to support all critical systems. **Responsibility: Facilities Manager**

3.3.5 All UPS equipment, air conditioning and fire detection/suppression equipment Must be regularly tested and maintained in accordance with the manufacturer's recommendation. **Responsibility: Facilities Manager**

Equipment Security on-site

3.3.6 IS equipment must be protected or located in such a manner that reduces the Risks of unauthorized access, hazards and accidental damage. The following procedures should be adhered to when considering the security of equipment on-site

Smoking, eating and beverages are prohibited in IS Equipment areas. **Responsibility: Facilities Manager**

Fire, smoke, water, dust, vibration, chemical Vapours and electromagnetic field must be taken Into consideration when identifying potential Hazards. **Responsibility: Facilities Manager**

Equipment Security off-life

3.3.7 IS equipment used off-site to support operational activities, or any other Purpose, must be subject to an equivalent level of security afforded on-site. The following precautions should be adhered to:

All computers must have virus controls in place. The Anti-virus software is to comply with Fort Hare standard. **Responsibility: LAN/PC Manager**

When traveling, IS equipment must not be left unattended in a public place. Laptop computers are to be carried as hand luggage when traveling. **Responsibility: All Users**

Laptop computers must be protected with a BIOS password to prevent unauthorized access. **Responsibility: LAN/PC Manager**

All computers used off-site are not to be configured in any way to join other networks without the permissions of the head of Information Technology.
Responsibility: All users

All security practices outlined in section 1 on Authentication and Identification are to be complied with.
Responsibility: LAN/PC Manager

3.4 Logical Access Security – Standard

3.4.1 The standard operating encryption feature is to used encrypt all dial-up sessions.

3.4.2 Network Associates McAfee Enterprise Edition is the Fort Hare standard anti-virus software and will be loaded on all computers owned by Fort Hare. This includes all standalone computer located on and off-site.

3.4.3 The latest version of the anti-virus software is to be rolled out and used at all times. In the case of standalone computers, the version is to be upgraded on a monthly basis

3.5 Logical Access Security – Procedures

Requests for Additional Privileges

3.5.1. Existing network users requesting additional access privileges are to complete a

"User Changes" form and forward it to the Information Technology department once It has been completed appropriately. **Responsibility: All Users**

3.5.2 The approved form is then to be forwarded to the System Administrator for the Additional privileges to be granted

Management of User Access

3.5.3 The system Administrator is responsible for granting access to fort hare ICT infrastructure. **Responsibility: System Administrator**

3.5.4 The level access granted to the user must be appropriate for the corresponding function. **Responsibility: System Administrator and Information Custodian and Owner**

3.5.5 System Access privileges of users who have changed roles or who have left fort hate will be immediately revoked. **Responsibility: System Administrator**

3.5.6 Users requiring relief from all or part of their role for an extended period should fill out a "User Changes" form specifying the start and end dates of the relief period and the level access to be granted to the individual performing the relief. The form is to be forwarded to the ICTS department for approval. **Responsibility: System Administrator and User**

3.5.7 All user Ids that have not been used for more than 60 days will be regarded as redundant and will have their system access privileges revoked. **Responsibility: System Administrator**

3.5.8 A logon warning notice must be displayed on all computer screens with an appropriate legal warning regarding unauthorized access

3.5.9 A minimum level of system access is to be provided to contractors and consultants, unless a valid business case can be presented. **Responsibility: System Administrator and Information Owner**

Application Access Control

3.5.10 The Information Owner is responsible for granting appropriate application access. **Responsibility: Information Owner**

3.5.11 A "User Changes" form is to be completed and forwarded to the Information Technology department for approval. The form is the sent to the System Owner, who will decide on the appropriate level of access to the required application. **Responsibility: System Administrator and User**

3.5.12 Application system should control user access to data and application system functions in accordance with this and other relevant security policies. **Responsibility: Information Custodian**

3.5.13 Strict control should be maintained over access to program source libraries in order to minimize the corruption of computer programmers. **Responsibility: Information Custodian**

3.5.14 The system Administrators should review all access to applications every 3 months to ensure that these remain appropriate and that all defined users remain valid. **Responsibility: System Administrator**

3.5.15 Access to application system should not in any way compromise the security of other system with which IT resources are shared. **Responsibility: Information Custodian and System Administrator**

3.5.16 Users who require a high level of system privilege e.g. Superusers should be issued with two user Ids. One of these is to be used for normal business use; the other is only to be used when the special privileges are required e.g. the creation of new users for applications. **Responsibility: System Administrator**

Database Access Control

3.5.17 Users will access the database via the application front-end or via standard reporting tools after valid user ID and password have been entered. Attempts to access the database by any other means will be subject to investigation. **Responsibility: Information Custodian and System Administrator**

3.5.18 The information owners should review all privileges of users with access to database every 6 months to ensure appropriateness and that all defined users remain valid. **Responsibility: Information Owner**

3.5.19 Information Owner requiring access to application databases for report writing should be granted read-only access. **Responsibility: Information Owner**

Requests for Access to University of Fort Hare ICT Infrastructure (New Users)

3.5.20 "User Access Request" forms for access to the ICT infrastructure are to be completed during the Orientation programmer for both staff and students. **Responsibility: User**

3.5.21 The form is to be approved by a head of Department and the forwarded to the Information Owner. **Responsibility: Head of Department and Information Owner**

3.5.22 The Information Owner will review the application for completeness and appropriateness before the level of access is decided on and the account is created by the System Administrator. **Responsibility: Information Owner**

3.5.23 The ICTS department will then be requested to assign the level of access. **Responsibility: ICTS Department**

3.6 **Remote Access – Procedures**

3.6.2 Remote access to the Fort Hare ICT infrastructure is only to be granted to authorize Users. Application for remote access is to be dealt with in the same way as Applications for access to the fort hare ICT infrastructure (Refer to 2.2)

3.6.3 All remote access to the fort hare IT infrastructure is subject to the following:

All access and activity on the system is to be logged. **Responsibility department. System Administrator**

The remote access logs will be reviewed and any suspicious activity or security breaches will be reported to the head of ICTS

3.6.4 All user Ids and passwords are to adhere to the criteria outlined above detailing "password Use" (refer 1.2)

3.6.5 The entire remote access session will be encrypted. This includes the initial authentication process and all data transmission thereafter. **Responsibility: System Administrator**

3.6.6 The remote access callback facility will be enforced wherever possible. **Responsibility: System Administrator**

3.6.7 All users provided with remote access should be reviewed every three months by the information owners in order to ensure that all users are valid and require this access. **Responsibility: System Administrator**

3.6.8 Remote access rights of users, third party users and contractors who leave the employment, or registration of fort hare will be terminated immediately with effect from their date of departure. **Responsibility: System Administrator**

3.6.9 Modems may not be installed without a valid business purpose. The system Administrator, in conjunction with the Information Technology department, must first approve the installation of a modem. **Responsibility: IT department/System Administrator**

4 Availability

4.1 Objectives

The availability of Fort Hare ICT Infrastructure and other systems is important in order to provide continued and uninterrupted operations. Adequate procedures addressing virus control, data backup, security breaches, equipment maintenance and redundancy are therefore essential to ensure this availability.

4.2 Principles

4.2.1 All procedures designed to minimize the risk of data loss through computer virus infections must be strictly adhered to in order to ensure the availability of fort hare ICT Infrastructure.

4.2.2 All data located on the ICT infrastructure and other systems, which is the responsibility of the ICTS Department, is to be backed up. Users are responsible for backing up data located on their computers.

4.2.3 All breaches of security are to be reported to the Help Desk of the ICTS department as soon as possible and handled according to defined procedures.

4.2.4 All ICT assets and resources are to be maintained in accordance with the manufacturer's requirements. This ensures maximum life span of assets and resources.

4.2.5 Where possible, the use of redundant solutions is to be used; Redundancy of system ensures continued availability.

4.3 Protection from Malicious Software (viruses) – Procedures

Minimising the risk of a virus infection

4.3.1 All media introduced to fort hare infrastructure/network must be scanned for viruses. **Responsibility: System Administrator**

4.3.2 It is the responsibility of the System Administrator to ensure that all third party users Logging onto fort hare network use the standard anti-virus software. **Responsibility : System Administrator**

4.3.3 Users may not transfer or use software from any location outside fort hare ICT infrastructure without proper authorization from a Head of Department or the System Administrator. **Responsibility: Users**

4.3.4 No user may disable, remove or re-configure the standard anti-virus software in any way. **Responsibility: User**

4.3.5 All files downloaded from the Internet will be scanned by the fort hare firewall. **Responsibility: User and System Administrator**

Responding to a virus infection

4.3.6 If a virus is found, the following procedures should be followed: **Responsibility: All**

The occurrence should be logged with the Help Desk and the nature of the incident should be recorded (e.g. date, time, location, name/description of virus, suspected source, whether it was

successfully cleaned by the anti-virus software, extent and type of damage, etc).

If the anti-virus software is not able to disinfect and clean the affected computer, an ICTS staff member will be informed and proceed with the cleaning and recovery process.

Users must not attempt to eradicate the virus unless they do so while in communication with an ICTS staff member. This communication will help minimize damage to data files and software, as well as ensure that information needed to detect a reinfection has been recorded.

A report summarising all logged malicious software activity is to be prepared by the ICTS department.

4.4 Data backup – Procedures

Server backup

4.4.1 It is the responsibility of the ICTS Department to backup all critical data located on servers in accordance with defined and documented procedures. **Responsibility: System Administrator and ICTS department**

4.4.2 At least two generations of backup tapes must be stored off-site, in a physically secure and fireproof environment. Records of backup logs must be stored in a similar fashion to the backup tapes. **Responsibility: System Administrator and ICTS department**

4.4.3 A full backup of the system must be performed upon the initial installation of any system component and before and after any system changes. **Responsibility: System Administrator and ICTS department**

4.4.4 Data backups should be regularly tested to ensure that they can be relied upon for emergency use. **Responsibility: System Administrator and ICTS department**

Workstation backup

4.4.5 It is the responsibility of the user to backup important data to the user area on the server on a regular basis. **Responsibility: User**

4.4.6 The ICTS Department will not be held accountable for the loss of important data located on the hard disks of workstation computer. **Responsibility: User**

4.5 Breaches of Security – Procedures

4.5.1 All suspected or actual breaches of security must be reported to the helpdesk. **Responsibility: All**

4.5.2 The helpdesk will forward all matters relating to a suspected or actual breach of security to the head of information technology who will assess the severity of the situation and make a decision on whether to seek external assistance. **Responsibility: ICTS Helpdesk**

4.5.3 The head of ICTS will co-ordinate all activities related to a breach in fort hare information security. **Responsibility: Head of ICTS**

4.6 Maintenance of Equipment – Procedures

4.6.1 All fort hare IS assets and resource should be correctly maintained in accordance with supplier's recommendations to ensure its continued availability and integrity. **Responsibility: System Administrator and Information Custodian**

4.6.2 External companies responsible for the maintenance of hardware will be required to comply with the above procedure that will be enforced using contracts or Service Level Agreements (SLAs). **Responsibility: Information Custodian and External parties**

4.7 Redundancy – Procedures

4.71 In order to ensure the continued operation and availability of critical systems, a fault Tolerant/redundant design is to be used where possible. **Responsibility: System Administrator and Information Custodian.** This includes

Dual processing
Disk mirroring
Database replication
Uninterrupted power supply (UPS)

4.7.2 Alternate communication links should be tested and used to ensure the continued availability of communications in fort hare. **Responsibility: System Administrator**

5. System Development and Maintenance

Objectives

Security countermeasures are both cheaper and more effective if identified and applied at the requirements phase of a project and justified, agreed and documented as part of the overall business case instead of being applied retrospectively

Principles

Before a new system is acquired or implemented, Head of Department or data owners must consult with the head of ICTS in order to specify the security requirements. Alternatives must be reviewed with vendors and implementation consultants so that an appropriate balance is struck between security and other objectives (ease-of –use, operational simplicity, ability to upgrade, acceptable cost, etc). **Responsibility: Heads of department or data owner.**

All software testing and training for system must be accomplished exclusively with sanitized test data.

Application software developers must not have access to the live envirinment.
Responsibility: Software developer.

New application software still in the implementation phase must be kept strictly separate from live application software. If existing facilities permit it, this separation must be achieved via physically separate computer system.

6. System Change Control

Objectives

Formal change control procedures increase the quality, efficiency and security of the data to the processed and promote stability during the implementation phase of information system.

Principles

The change control must not compromise the existing security of the fort hare ICT infrastructure and standalone systems

All changes to systems must be documented, tested and approved in a controlled and systematical manner before implementation.

All intermediate and final products of the systems development process either purchased or developed at the direction of fort hare are the exclusive property of fort hare and are solely for fort hare use.

Fort hare management must ensure that all development and maintenance activities (hardware, software and infrastructure) by both external companies and in-house, subscribe to fort hare change control principles, standards and procedures.

7. Auditing, Logging and Monitoring

Objectives

To ensure that any activity that constitutes breach of fort hare ICT infrastructure will be detected using audit trails, event logging and monitoring. This will help to minimize the risk of unauthorized use, abuse and entry.

Principals

Fort hare ICT infrastructure and other system must be monitored on an ongoing basis for security violations and suspicious activity.

Any security breaches detected by the standard auditing, logging and monitoring tools will be addressed within eight working hours. An investigation will be launched should this time period elapse.

Fort hare reserves the right to monitor all traffic on the fort hare network. Any or all users, PCs, terminals, network addresses, user ID's email or other network traffic may be monitored at any time for compliance with security controls and policy.

Procedures

The system Administrator and Information Owners must enable system logging and auditing functions and must ensure that the audit logs are audit logs are protected from unauthorized access. **Responsibility: System Administrator and Information and Information Owner.**

It is the responsibility of the System Administrator, System Owners, Database Administrator and the head of ICTS to monitor the fort hare ICT infrastructure and standalone systems for attempts to circumvent system security. **Responsibility: System Administrator, Information Owner, Database Administrator and head of ICTS**

Audit trails recording exceptions and other security-related events should be produced and kept for an agreed upon period to assist in future investigations and access control monitoring. A record of rejected access attempts will be created. **Responsibility: System Administrator, Information Custodian.** At a minimum, audit trails will include:

User ID's
Dates and times for logon and logoff
Terminal identity or location if possible

Configurations of system should be monitored in order to identify any changes and investigate all anomalies. **Responsibility: System Administrator and Information Custodian**

Audit trails must be reviewed weekly and kept for an agreed period to assist in future investigations and access control monitoring. **Responsibility: System Administrator and Information Custodian**

All staff and students of fort hare are responsible for maintaining a familiarity with the information security policies, standards and guidelines and are responsible for reporting any suspected security breaches or violations. **Responsibility: User**

The use of automated tools to facilitate review audit data on a frequent basis is strongly recommended. Additionally, to ensure the accuracy of audit logs, system clocks should be synchronized across the network. **Responsibility: System Administrator and Information Custodian.**

8. Documentation

Objectives

It is essential that relevant and up-to-date documentation is maintained to ensure that a common understanding of information security procedures, operational procedures, applications, systems and technologies are understood and in line with management expectations.

Principals

Documentation must be readily available and kept up-to-date for appropriate personnel in order to enhance job performance.

Procedures

Procedures must be written for the following items **Responsibility: Head of ICTS:**

Documentation relating to security incidents and how these are resolved
General operating procedures
Application documentation, together with changes that have been made
Disaster Recovery Plan
Business Continuity Plan
Detailed system restart and recovery procedures for use in the event of System failure
Database-specific administration procedures
Acceptable use procedures for all application and systems present at fort Hare.

Other corporate policies, standards and guidelines, including but not limiting, the following **Responsibility: Head of ICTS**

Detailed backup and recovery policy
System development policy
Change control policy

Approved on behalf of Council: _____

Vice Chancellor: Dr. Mvuyo Tom