INFORMATION SECURITY MANAGEMENT POLICY

Policy Code: C3
Version: 1
Approved by: EXCO
Approval Date: 30/06/2021
Decision No.: EXCO39/2021

Date Reviewed	Version History
25/06/2021	V1

Contents

1. INTRODUCTION

The Institute is an accredited private higher distance education provider offering qualifications on NQF levels five to ten, which are registered on the Higher Education Qualifications Sub-Framework (HEQSF). This policy forms part of the institutional Integrated Quality Management System and details the principles for ensuring that programme offerings adhere to academic standards and empower students to contribute to the transformation of their communities, society, and the economy of the future. This approach is underpinned by the Business- and Community-based Action Learning discourse on the co-creation and distribution of relevant knowledge.

The Management of The Institute for Higher Education is committed to preserving the confidentiality, integrity and availability of all of its physical and electronic information assets in order to sustain its competitive advantage, cash-flow, profitability, legal, regulatory and contractual compliance as well as its commercial image. The Institute's information security requirements are aligned with these goals. The violation of technology information exposes The Institute to legal risks and liability.

This Policy provides the requirements to ensure that the security of The Institute's information, data, records and documents are upheld. It also details The Institute's approach to Information Technology (IT) security management based upon the *International Organization for Standardization ISO27002* standards, the code of practice for corporate information security management. The Institute is committed to the development and maintenance of its Information Security Management System (ISMS).

2. ACRONYMS

IT	Information Technology
ISMS	Information Security Management System

3. DEFINITIONS

Term	**Definition**
Access Control	The rules and deployment mechanisms which control access to information systems, and physical access to premises. The entire subject of information security is based upon access control, without which information security cannot, by definition, exist
Audit Logs	Files containing details of amendments to records, which may be used in the event of system recovery being required. The majority of commercial systems feature the creation of

Term	Definition
	an audit log. It permits subsequent review of all system activity, and provides details of which user ID performed which action to which files, when, etc.
Authentication	The verification of the authenticity of either a person or of data, e.g. a message may be authenticated to have been originated by its claimed source. Authentication techniques usually form the basis for all forms of access control to systems and/or data
Communication System	Facilities made available by The Institute or allowed for business purposes which include, but not limited to Internet access, email access and use of any equipment for purposes of: i. Accessing, creating, copying, distributing, sharing and deleting records ii. Initiating, creating, receiving or storing communications.
Confidential Information	Privileged, sensitive information which concerns or relates to the trade secrets, processes, operations, style of works, or to the production, sales, purchases, transfers, identification of customers, inventories, or amount, or source of any income, profits, losses
DSS (Data Security Standards)	Data Security Standards as prescribed by the Payment Card Industry (PCI)
Dual Control	A control procedure whereby the active involvement of two people is required to complete a specified process.
Encryption	The process by which data is temporarily re-arranged into an unreadable or unintelligible form for confidentiality, transmission, or other security measures
Equipment	Computers, desktops, servers, routers, laptops, telephones, networks, cell phones, electronic handheld devices, facsimile machines, pagers, software, hardware and/or similar equipment owned by, licensed to, or rented by The Institute, or user equipment that is utilised by users of The Institute's information systems
Error Log	A log of any abnormal activity on application software, usually in simple/plain text. Each main application generates its own logs, and it is the responsibility of systems operations to retrieve and scrutinise this for any processing errors
Firewalls	Are security devices used to restrict access in communication networks. Firewalls prevent computer access between networks, for example from the internet to the user (corporate network), and only allows access to

Term	Definition
	services which are expressly registered. Firewalls also keep logs of all activities, which may be used in investigations
Information Asset	A definable piece of information, stored in any manner which is recognised as 'valuable' to the organisation. The information which comprises an information asset may be little more than a prospect name and address file; or it may be the plans for the release of the latest in a range of products to compete with competitors
Information Security department	The persons appointed and employed by The Institute to enforce and manage information security matters
ISO (International Organization for Standardization)	ISO/IEC 27002 is an information security standard published by the *International Organization for Standardization* (ISO), and by the *International Electrotechnical Commission* (IEC), titled, *Information technology – Security techniques – Code of practice for information security management*
Mobile Storage Devices	Any data storage unit, and includes, but is not limited to Flash Cards, Flash Disks (memory sticks), Tapes, Drives, CDs, CD Writers, DVDs and DVD writers
Operating System	Computer programmes that are primarily or entirely concerned with controlling a computer and its associated hardware, rather than with processing work for users. Computers can operate without application software, but cannot run without an operating system
PCI (Payment Card Industry)	Is a proprietary information security standard for organisations that handle branded credit cards from the major card schemes
Policy	A statement of management philosophy and direction, established to provide guidance and assistance to the institution's community in the conduct of its affairs
Removable Media	Any data storage unit that can be removed from the equipment and The Institute's premises, and includes, but is not limited to Flash Cards, Flash Disks (memory sticks), Tapes, Drives, CDs, CD Writers, DVDs and DVD writers
SLA (Service Level Agreement)	Is a contract between The Institute and the vendor of the system(s) to provide a range of support services, up to an agreed minimum standard. SLAs will specify precisely what the support procedures are to be, and the way in which a support call will be escalated to the vendor's support organisation to achieve resolution
UPS (Uninterrupted Power Supply)	A UPS is a device that provides consistent backup power during inconsistent power issues. The UPS can protect both data and the computer equipment connected to it by stabilising the voltage passing through. A power 'outage' or

Term	Definition
	a surge can shut down the communication systems within seconds. If this happens on a Windows® PC, the consequence is the loss of the files that the users were currently working on. If the server has the power cut, the consequences can be more serious, as potentially hundreds of files can be left in an 'open' state which, in the worst scenario, could prevent the system from rebooting properly - or even at all
User Requirement Specification	Is a document produced by, or on behalf of the organisation which documents the purposes for which a system is required; its functional requirements, usually in order of priority/gradation
Virus	Is a form of malicious code and, as such, it is potentially disruptive. It may also be transferred unknowingly from one computer to another. The term virus includes all sorts of variations on a theme, including the nastier variants of macro-viruses, Trojans and Worms. For convenience, all such programmes are classed simply as 'virus'

4. REGULATORY FRAMEWORK

The Information Security Management Policy is benchmarked against, and should be read in the context of the relevant legislation underpinning the principles against which institutional policies, processes and standard operational procedures are developed, implemented and maintained. These include:

A. Relevant legislation

I. Constitution of the Republic of South Africa (No.108 of 1996)
II. Electronic Communications and Transactions Act (No.25 of 2002)
III. Films and Publications Act (No.65 of 1996)
IV. Promotion of Access to Information Act (No.2 of 2000)
V. Protection of Personal Information Act (No.4 of 2013)

B. Applicable Da Vinci documents:

I. A7 - Communications
II. A12 - Records Management Policy
III. B25 - Social Media Policy
IV. C1 - Electronic Information and Communication System Policy
V. C2 - Acceptable Use of Information Policy
VI. C4 – Firewall Policy
VII. C5 - Wireless Communication Policy

VIII. C6 - Change Management Information Technology Policy
IX. C7 - Incident and Service Management Information Technology Policy
X. C8 - Disaster Recovery Information Technology Policy
XI. C9 – Backup Policy
XII. C11 - Data Breach Policy
XIII. PAIA Manual
XIV. Records Retention Schedule

5. SCOPE

This policy applies to all The Institute's employees and other persons who have access to, and use The Institute's equipment to create, access or use The Institute's information and systems, and forms part of the ISMS, including, but not limited to:

a) Employees
b) Elected Members
c) Contractors
d) Temporary staff
e) Partner organisations
f) Customers
g) Members of the public
h) Volunteers
i) Any other party utilising The Institute's IT resources.

6. POLICY STATEMENT

This policy is based on the principles set out in the *International Organization for Standardization ISO27002*. The Institute is committed to ensuring appropriate controls and security measures for all information technology systems and electronic information under its control. However, this is not enough, and every person that uses, provides, or administrates information resources, has a responsibility to maintain and safeguard these assets. Each authorised user at The Institute is expected to be informed, responsible for, protecting their own information resources in any environment, shared or stand-alone, and using these shared resources to consider others. The following aspects relating to security are included in the policy:

.

a) Providing direction and support for IT security in accordance with business requirements, regulations and legal requirements
b) Stating the responsibilities of staff, partners, contractors and any other individual or organisation having access to The Institute's IT systems
c) Stating management intent to support the goals and principles of security in line with business strategy and objectives
d) Providing a framework by which the confidentiality, integrity and availability of IT resources can be maintained

e) Optimising the management of risks, by preventing and minimising the impact of IT security incidents
f) Ensuring that all breaches of IT security are reported, investigated and appropriate action taken where required
g) Ensuring that supporting IT security policies and procedures are regularly reviewed to ensure continued good practices and protection against new threats
h) Ensuring IT information security requirements are regularly communicated to all relevant parties.

7. PURPOSE

The purpose of this policy is to outline the requirements to:

a) Protect The Institute's business information and any client or customer information within its custody or safekeeping by safeguarding its confidentiality, integrity and availability, which could include data and information that is:

I. Stored on databases
II. Stored on computers
III. Transmitted across internal and public networks
IV. Printed or hand-written on paper, white boards, 'black books', etc.
V. Sent by facsimile (fax), telex or other communication methods
VI. Stored on removable media
VII. Stored on fixed media such as hard disks and disk sub-systems
VIII. Stored on Cloud storage
IX. Held on film or microfiche
X. Created, stored or distributed through the use of electronic communication facilities
XI. Presented on slides and overhead projectors, using visual and audio media
XII. Spoken during telephone calls and meetings, or conveyed by any other method.

b) Establish safeguards to protect The Institute's information resources from theft, abuse, misuse and any form of damage
c) Establish responsibility and accountability for information security at The Institute
d) Encourage management and staff to maintain an appropriate level of awareness, knowledge and skill to allow them to minimise the occurrence and severity of information security incidents
e) Ensure that The Institute is able to continue its commercial activities in the event of significant information security incidents
f) Provide suitable coverage according to *International Standards ISO 17799* best practices for control objectives, and controls for information security management, and Payment Card Industry (PCI) DSS policies and procedures.

8. RESPONSIBILITIES AND DUTIES

a) Co-ordination of information security management across the institution through an internal information governance framework is headed by the Head of Information and Communication Technology.
b) Duties include:

I. Develop information security policies and procedures
II. Monitor information security activity and compliance
III. Administer an annual self-assessment compliancy questionnaire
IV. Establish business continuity plans
V. Respond to information security incidents
VI. Audit and review security procedures
VII. Allocate information security responsibilities
VIII. Educate and train users on security matters.

c) Day-to-day responsibility for the management of ISMS and information may be delegated to staff designated as information or system owners within departments
d) It is the responsibility of every individual of the organisation having access to The Institute's ISMS and information, to comply with this policy, associated criteria and procedures, and to take adequate steps to safeguard the security of the equipment and information to which they have access. Any suspected or actual security weakness, threats, events or incidents must be immediately reported to the Head of Information and Technology via the Incident Reporting system.

9. HARDWARE AND EQUIPMENT SECURITY

9.1. Purchase and installation

a) All purchases of new systems hardware or new components for existing systems must be made in accordance with The Institute's information security, finance and other relevant policies, as well as the required technical standards. Such requests to purchase must be based upon user requirement specifications considering longer term business needs
b) All new hardware installations are to be planned formally and notified to all interested parties ahead of the proposed installation date. Information security requirements for new installations are to be circulated for comment to all interested parties
c) All equipment must be fully and comprehensively tested and formally accepted by users before being transferred to the live environment, taking into consideration applicable policy requirements.

9.2. Cabling, printers and modems

a) A UPS is to be installed to ensure the continuity of services during power outages
b) Secondary and backup power generators are to be employed where necessary to ensure the continuity of services during power outages
c) Sensitive or confidential information may only be faxed where more secure methods of transmission are not feasible
d) Both the owner of the information and the intended recipient must authorise the transmissions beforehand. Recipients are preferably to be present at the fax facility to receive such communications
e) Sensitive or confidential information may only be sent via public telephone lines where more secure methods of transmission are not feasible. Both the owner of the information and the recipient must authorise the transmission beforehand
f) Information classified as 'Sensitive Information', 'Confidential Information', 'Highly Confidential Information' or 'Trade Secret' may never be sent to a network printer without there being an authorised person to safeguard its confidentiality during and after printing
g) Network cabling should be installed and maintained by qualified engineers to ensure the integrity of both the cabling and the wall-mounted sockets. Any unused network wall sockets should be sealed-off and their status formally noted.

9.3. Consumables

a) IT consumables must be purchased in accordance with The Institute's approved purchasing procedures with usage monitored, to discourage theft and improper use
b) Only personnel who are authorised to install or modify software shall use removable media to transfer data to/from The Institute's network. Any other persons shall require specific authorisation.

9.4. Working Remotely (Off-premises)

a) Line management must authorise the issue of portable computers
b) Usage is restricted to business purposes, and users must be aware of, and accept the terms and conditions of use, especially responsibility for the security of information held on such devices
c) Persons who are issued with portable computers and who intend to travel for business purposes must be made aware of the information security issues relating to portable computing facilities and implement the appropriate safeguards to minimise the risks to safeguard such information
d) Off-site computer usage, whether at home or at other locations, may only be used with the authorisation of line management

e) Usage is restricted to business purposes, and users must be aware of, and accept the terms and conditions of use, which must include the adoption of adequate and appropriate information security measures
f) Any movement of hardware between The Institute's locations is to be strictly controlled by authorised personnel
g) Laptop computers are to be issued to, and used only by authorised employees and only for the purpose for which they are issued. The information stored on the laptop is to be suitably protected at all times.

9.5. Hardware maintenance

a) Warranties of all purchased equipment should be stated and maintained in the Hardware Asset register
b) All equipment owned, leased or licensed by The Institute must be supported by appropriate maintenance facilities from qualified engineers
c) Only suitable and approved cleaning materials are to be used on equipment owned by The Institute
d) Deliberate or accidental damage to The Institute's property must be reported to the Head of Information and Communication Technology as soon as it is noticed.

9.6. Hardware disposal

a) Equipment owned by The Institute may only be disposed of by authorised personnel who have ensured that the relevant security risks have been mitigated
b) All information system hardware faults are to be reported promptly and recorded in a Hardware Fault Register
c) All computing equipment and other associated hardware belonging to The Institute or leased from third parties must carry appropriate insurance cover against hardware theft, damage, or loss
d) All portable computing equipment is to be insured to cover travel domestically or abroad
e) Approved login procedures must be strictly observed and users leaving their screen unattended must firstly lock access to their workstation or log off
f) Sensitive or confidential Information must not be recorded on answering machine/voice mail systems
g) Only authorised personnel are permitted to take equipment belonging to The Institute off the premises; they are responsible for its security at all times. Removal of equipment shall only be allowed, subsequent to the signing of the necessary release form made available by the IT department
h) All speed dialling systems must incorporate security features which protect sensitive or confidential information.

9.7. Paper trail

a) Hardware documentation must be kept up-to-date and readily available to the staff who are authorised to support or maintain systems
b) A formal inventory of all equipment is to be maintained and kept up to date at all times, with specific reference to any warranties that may be applicable.

9.8. Secure storage

a) Sensitive or valuable material and equipment must be stored securely and according to the classification status of the information being stored
b) Documents are to be stored in a secure manner in accordance with their classification status.

10. ACCESS CONTROL

a) Access control standards for information systems must be established by the Head of Information and Communication Technology
b) Access control standards should incorporate the need to balance restrictions to prevent unauthorised access against the need to provide unhindered access to meet business needs
c) Access to all systems must be authorised and such access, including the appropriate access rights (or privileges) must be recorded in an Access Control Register. Such records are to be regarded as 'highly confidential' and safeguarded
d) Equipment is always to be safeguarded appropriately, especially when left unattended
e) Access to the resources on the network and cloud services must be strictly controlled to prevent unauthorised access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised. These measures are in place to ensure that only authorised users are able to perform actions or have access to information on institutional systems and servers, as well as on PCs and devices used by individuals or groups
f) Appropriate firewalls should be installed and firewall configuration to be maintained according to the Firewall Policy
g) Access to operating system commands is to be restricted to those persons who are authorised to perform systems administration/management functions. Even then, such access must be operated under dual control requiring the specific approval of senior management
h) 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. In particular, passwords shall not be shared with any other person for any reason
i) No vendor-supplied defaults for system passwords and other security parameters should be used

j) Physical access to high security areas is to be controlled with strong identification and authentication techniques. Staff with authorisation to enter such areas are to be provided with information of the potential security risks involved
k) Access controls are to be set at an appropriate level which minimises information security risks, yet also allows The Institute's business activities to be carried out without undue hindrance
l) Access is to be logged and monitored to identify potential misuse of systems or information
m) Access to information and documents is to be carefully controlled, ensuring that only authorised personnel may have access to 'sensitive Information', confidential information' and 'highly confidential information' or trade secrets
n) Access controls for information or high risk systems are to be set in accordance with the value and classification of the information assets being protected
o) Remote and cloud access control procedures must provide adequate safeguards through robust identification, authentication and encryption.

11. PROCESSING INFORMATION AND RECORDS

11.1. Networks

a) The network must be designed and configured to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and a range of privilege restrictions. Network high delivery and availability is largely determined by Microsoft 365 and cloud network infrastructure and everyone's connectivity and reliability
b) Suitably qualified staff are to manage The Institute's network and preserve its integrity in collaboration with the nominated individual system owners
c) Remote access to The Institute's network and resources will only be permitted providing that authorised users are authenticated, data is encrypted across the network, and privileges are restricted
d) System hardware, operating and application software, the networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised network intrusion
e) Network scans must be conducted by a qualified third party service provider, alternatively a PCI Approved Scanning Vendor (ASV) and scan reports must be made available for inclusion in the annual Self-assessment Compliancy Questionnaire.

11.2. System Operations and Administration

a) The Institute's systems are to be managed by a suitably qualified systems administrator of The Institute who is responsible for overseeing the day-to-day running and security of the systems

b) System Administrators must be fully trained and have adequate experience in the wide range of systems and platforms used by The Institute. In addition, they must be knowledgeable and conversant with the range of information security risks which need to be managed
c) For authorised personnel, the appropriate data and information must be made available as and when required, for all other persons, access to such data and information is prohibited, with appropriate technical control required to supplement the enforcement of this policy
d) Third party access to corporate information is only permitted where the information in question has been 'ring-fenced' and the risk of possible unauthorised access is considered to be negligible
e) The management of electronic keys to control both the encryption and decryption of sensitive messages must be performed under dual control, with duties being rotated between staff
f) The Institute's systems must be operated and administered using documented procedures in a manner which is both efficient, but also effective in protecting The Institute's information security
g) System documentation is a requirement for all The Institute's information systems. Such documentation must be kept up-to-date and be available when required
h) Error logs must be properly reviewed and managed by qualified staff
i) Systems Operations schedules are to be formally planned, authorised and documented
j) Changes to routine systems operations are to be fully tested and approved before being implemented
k) Operational audit logs are to be reviewed regularly by trained staff and discrepancies reported to the owner of the information system
l) System clocks must be synchronised regularly especially between The Institute's various processing platforms
m) Only qualified and authorised staff or approved third party technicians may repair information system hardware faults
n) Transaction and processing reports should be regularly reviewed by properly trained and qualified staff
o) Any organisation accessing The Institute's systems or network must be able to demonstrate compliance with The Institute's policy requirements under its ISMS.
p) Staff responsible for setting up internet access are to ensure that The Institute's network is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall according to the requirements of the Firewall Policy. All personnel with internet access and e-mail must be aware of the acceptable use and security requirements, and comply with The Institute's various information technology, systems and communication system policies when utilising internet services
q) Computer files received from unknown senders are to be deleted without being opened

r) Any fax or e-mail received in error is to be returned to the sender. Its contents must not be disclosed to other parties without the sender's permission
s) Staff authorised to make payment by credit card for goods ordered over the telephone, are responsible for safe and appropriate use of the system.

12. DATA MANAGEMENT

12.1. Storing data

a) Sensitive, confidential data, information or trade secrets, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured, for example, by using encryption techniques
b) The identity of persons requesting sensitive or confidential information or trade secrets must be verified, and they must be authorised to receive it
c) Day-to-day stored data needs to be readily available to authorised users and archives must be created and accessible in case of need
d) The integrity and stability of The Institute's databases must be maintained at all times
e) Emergency data amendments may only be used in extreme circumstances, and only in accordance with emergency amendment procedures
f) The use of mobile storage devices is allowed provided it is thoroughly scanned for viruses
g) Data directories and structures should be established by the owner of the information system with users adhering to that structure. Access restrictions to such directories should be applied as necessary to restrict unauthorised access
h) Existing directory and folder structures may only be amended with the appropriate authorisation from the owner of the information system concerned
i) Third party service providers for purposes of processing data shall only be utilised subsequent to:

    I. Service provider contingency and disaster recovery procedures that have been assessed
    II. Service provider agreement to the management of data in a manner similar to the conditions/principles stated in data protection legislation applicable to The Institute
    III. Charge for extra storage back-up and cloud-to-cloud for business continuity have been reviewed and accepted
    IV. Appropriate service levels have been established
    V. The service provider has established acceptable procedures that will be applicable during any data breach or compromise
    VI. Service provider agrees to return, alternatively destroy data that are in its possession at expiration or termination of the service agreement

VII. Security assessment in terms of the third party has been done
VIII. Written agreements have been signed.

j) The archiving of documents must take place with due consideration for legal, regulatory and business issues with liaison between technical and business staff
k) The information created by, and stored on The Institute's information systems must be retained for a minimum period that meets both legal and business requirements according to The Institute's A12: Records Management Policy.
l) The classification of spreadsheets must be appropriate to the sensitivity and confidentiality of data contained therein. All financial/data models used for decision-making are to be fully documented and controlled by the information owner
m) Databases must be fully tested for both business logic and processing, prior to operational usage. Where such databases are to contain information of a personal nature or sensitive nature, procedures and access controls must ensure compliance with necessary legislation according to the legislative references of this policy
n) Highly sensitive or critical documents must not rely upon the availability or integrity of external data files over which the author may have no control. Key documents and reports must be self-contained and contain all the necessary information
o) Draft reports should only be updated with the authority of the designated owner of the report.
p) Draft version(s) of reports must be deleted or archived following production of a final version. A single version of the file should be retained for normal operational access.
q) Only authorised persons may access sensitive or confidential data on projects owned or managed by The Institute or its employees
r) Customer information may only be updated by authorised personnel
s) Customer data is to be safeguarded using a combination of technical access controls and robust procedures, with all changes supported by journal entries and internal audit controls
t) The naming of The Institute's data files must be meaningful and capable of being recognised by its intended users.
u) Temporary files on users' PCs and laptops are to be deleted regularly to prevent possible misuse by possible unauthorised users
v) Customer contact information is and secured according to The Institute's policies. Refer to *C2 – Acceptable Use of Information Systems*
w) All users of information systems whose job function requires them to create or amend data files, must save their work on the system regularly in accordance with best practice to prevent corruption or loss through system or power malfunction.

12.2. Back-up, Recovery and Archiving

a) Information system owners must ensure that adequate back-up and system recovery procedures are in place
b) Information and data stored on laptop or portable computers must be backed-up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis
c) Backup of The Institute's data files and the ability to recover such data is a top priority. Management is responsible for ensuring that the frequency of such back-up operations and the procedures for recovery meet the needs of the business
d) The storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must be carefully considered, especially where proprietary formats are involved
e) The archiving of electronic data files must reflect the needs of the business and also any legal and regulatory requirements
f) Management must ensure that safeguards are in place to protect the integrity of data files during the recovery and restoration of data files, especially where such files may replace more recent files.

12.3. Securing Data

a) Where required, sensitive or confidential information or data should always be transmitted in encrypted form. Prior to transmission, consideration must always be given to the procedures to be used between the sending and recipient parties, and any possible legal issues from using encryption techniques
b) Human Resources Management are to ensure that all employees are fully aware of their legal and corporate duties and responsibilities concerning the inappropriate sharing and releasing of information, both internally within The Institute and to external parties
c) Prior to sending information to third parties, not only must the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by the third party must be seen to continue to assure the confidentiality and integrity of the information
d) Information relating to the clients and third party contacts of The Institute is confidential, and must be protected and safeguarded from unauthorised access and disclosure
e) Customer credit card details entrusted to The Institute must be afforded a combination of security measures (technology and procedural) which, in combination, prevent all recognised possibilities of the card details being accessed, stolen, and modified, or any other way divulged to unauthorised persons

f) All data and information must be protected against the risk of fire damage at all times. The level of such protection must always reflect the risk of fire and the value and classification of the information being safeguarded
g) Prior to sending reports to third parties, not only must the intended recipient(s) be authorised to receive such information, but the procedures and information security measures adopted by each third party must be seen to continue to assure the confidentiality and integrity of the information
h) Sensitive financial information is to be classified as 'Highly Confidential' and must be afforded security measures (technology and procedural) which, in combination, safeguard such information from unauthorised access and disclosure
i) Data is to be protected against unauthorised or accidental changes, and may only be deleted with the proper authority
j) Sensitive/confidential electronic data and information should be secured with access control applied to the directory on the computer system concerned
k) The singular use of passwords to secure individual documents is less effective, and hence discouraged, as passwords may be either forgotten, or become revealed over time to unauthorised persons
l) Information classified as 'Highly Confidential' or 'Top Secret' may never be sent to a network printer without an authorised person at the printer to retrieve it, and hence safeguard its confidentiality during and after printing.

13. GENERAL INFORMATION HANDLING

a) The decision whether dual control is required for data entry is to be made by the information system owner. Where required, secure data handling procedures including dual input are to be strictly adhered to
b) Employees are not permitted to load non-approved screen savers onto The Institute's PCs and laptops
c) Any third party utilised for external disposal of The Institute's obsolete equipment and material must be able to demonstrate compliance with this policy under its ISMS and also, where appropriate, provide a Service Level Agreement which documents the performance expected, and the remedies available in case of non-compliance
d) The use of photocopiers for personal use is not allowed. In exceptional circumstances specific permission may be given by the employee's immediate manager
e) Only authorised personnel may speak to the media (newspapers, television, radio, magazines, etc.) about matters relating to The Institute, as per The Institute's *A7: Communication Policy* and *B25: Social Media Policy*.
f) Information regarding The Institute's customers or other people dealing with The Institute is to be kept confidential at all times. This information should only be released by authorised persons

g) The techniques of dual control and segregation of duties are to be employed to enhance the control over procedures wherever both the risk from, and consequential impact of a related information security incident would likely result in financial or other material damage to The Institute
h) The Institute expects all employees to operate a clear-desk policy to minimise information security risks
i) E-mail addresses and faxes are to be checked carefully prior to dispatch, especially where the information is considered to be confidential, and where the disclosure of the e-mail addresses or other contact information to the recipients is a possibility
j) The Institute values the integrity and correctness of all its business and related information and requires management to develop and adopt the appropriate procedures in this regard
k) Employees travelling on business are responsible for the security of information in their custody.

14. DOCUMENT HANDLING

a) Hard copies of sensitive or classified material must be protected and handled according to the distribution and authorisation levels specified for those documents
b) All employees are to be aware of the risk of breaching confidentiality associated with the photocopying (duplication) of sensitive documents
c) Authorisation from the document owner should be obtained where documents are classified as 'Highly Confidential'
d) All information used for, or by The Institute, must be filed appropriately and according to its classification
e) Documents should be checked and countersigned (either manually or electronically) to confirm their validity and integrity, especially those which commit or oblige The Institute in its business activities
f) All written communications sent out by The Institute to third parties are to be approved by authorised persons
g) All signatures authorising access to systems or release of information must be properly authenticated
h) Unsolicited mail should not receive serious attention until and unless the sender's identity and authenticity of the mail has been verified
i) The designated owners of documents which contain sensitive information are responsible for ensuring that the measures taken to protect their confidentiality, integrity and availability during and after transportation/ transmission, are adequate and appropriate
j) All documents of a sensitive or confidential nature are to be shredded when no longer required. The document owner must authorise or initiate this destruction
k) No document that contains sensitive or confidential or trade secret information may be removed from The Institute, unless authorised by the document owner.

15. CYBERCRIME

a) Security on the network is to be maintained at the highest level. Those responsible for the network and external communications are to receive proper training in risk assessment and how to build secure systems which minimise the threats from cyber-crime
b) Plans are to be prepared, maintained and regularly tested to ensure that damage done by possible external cybercrime attacks can be minimised, and that restoration takes place as quickly as possible
c) Perpetrators of cybercrime will be prosecuted by The Institute to the full extent of the law. Suitable procedures will be followed to ensure the appropriate collection and protection of evidence
d) In order to reduce the incidence and possibility of internal attacks, access control standards and data classification standards are to be periodically reviewed whilst maintained at all times
e) It is a priority to minimise the opportunities for cybercrime attacks on The Institute's systems and information through a combination of technical access controls and robust procedures
f) Risks to The Institute's systems and information are to be minimised by fostering staff awareness, encouraging staff vigilance, and deploying appropriate protective systems and devices
g) Without exception, antivirus software is to be deployed across all equipment with regular virus definition updates and scanning across both servers, PCs and laptop computers. The threat posed by the infiltration of a virus is high, as is the risk to The Institute's systems and data files. Formal procedures for responding to a virus incident are to be developed, tested and implemented. Virus incident responses must be regularly reviewed and tested
h) Anti-virus software must be chosen from a proven leading supplier. Windows Updates must be maintained to mitigate any other unauthorised entry to electronic equipment
i) Without exception windows updates must be deployed. All windows updates published must be run and should automatically be updated as required. Staff must frequently monitor that these updates and inform the IT department if updates are not working. Most of them include security updates that minimises the risk of malware and hacker exploits.

16. BUSINESS CONTINUITY

a) Management is required to implement a Business Continuity Plan should a business interruption have occurred

b) Management is to undertake a formal risk-assessment in order to determine the requirements and currency of the Business Continuity Plan.

17. COMPLIANCE BY STAFF AND THIRD PARTIES

a) The terms and conditions of employment of The Institute are to include requirements for compliance with The Institute's information security policies residing under its ISMS
b) New employees' references must be verified, and the employees must undertake to abide by The Institute's information security policies
c) All external suppliers who are contracted to supply services to The Institute must agree to comply with the information security requirements of The Institute according to its policies
d) An appropriate summary of The Institute's information security policies must be formally delivered to any such supplier, prior to any supply of services
e) Notwithstanding The Institute's respect for employee's privacy in the workplace, it reserves the right to have access to all information created and stored on The Institute's systems. All employee data is to be treated as strictly confidential and made available to only properly authorised persons
f) Management must respond quickly yet discreetly to indications of staff indiscretions, liaising as necessary with Human Resources and the Manager of Information and Technology
g) Employee meeting and interview records must be formally recorded, with the contents classified as 'Highly Confidential' and made available only to authorised persons
h) Upon notification of staff resignations, Human Resources must consider with the Manager of Information and Technology whether the member of staff's continued system access rights constitutes an unacceptable risk to The Institute, and, if so, revoke all access.

18. PREMISES

a) The Institute's sites including third party service provider sites chosen to locate computers and to store data must be suitably protected from physical intrusion, theft, fire, flood and other hazards
b) Computer premises must be safeguarded against unlawful and unauthorised physical intrusion
c) On-site locations where data is stored must provide access controls and protection which reduce the risk of loss or damage to an acceptable level
d) Remote locations where data is stored must provide access controls and protection which reduce the risk of loss or damage to an acceptable level
e) Electronic eavesdropping should be guarded against by using suitable detection mechanisms, which are to be deployed if and when justified by the periodic risk assessments of The Institute.

19. INCIDENT RESPONSE

a) All suspected information security incidents, weaknesses or breaches must be dealt with in accordance with the C7: Incident and Service Management Information Technology Policy.
b) All suspected information security incidents, weaknesses or breaches must be reported promptly to the appointed Manager of Information and Technology. Once the call has been entered into the system, an e-mail is generated and sent to the Manager of Information and Technology, and also copied to the Chief Executive Officer (CEO) who will then determine if the incident needs to be escalated to the appropriate pre-identified departmental representative to deal with. Representatives investigating security breaches will be responsible for updating, amending and modifying the status and clearance code of incidents in the call-logging system
c) Information security incidents must be reported to outside authorities whenever this is required to comply with legal requirements or regulations. This may only be done by authorised persons
d) Information security incidents must be properly investigated by suitably trained and qualified personnel
e) Evidence relating to an information security breach must be properly collected, taking into consideration evidential weight (electronic and physical evidence), and forwarded to the Manager of Information and Technology
f) A database of information security threats and remedial action should be available and maintained. This database should be studied regularly with the circumstantial evidence used to assist in reducing the risk and frequency of information security incidents at The Institute
g) The use of information systems must be monitored regularly with all unexpected events recorded and investigated. Such systems must also be periodically audited with the combined results and history strengthening the integrity of any subsequent investigations
h) Information security incidents arising from system failures are to be investigated by competent technicians.

20. TRAINING AND AWARENESS

a) Permanent staff are to be provided with information security awareness information to enhance awareness and educate them regarding the range of threats and the appropriate safeguards
b) An appropriate summary of the information security policies must be formally delivered to any contractor, prior to any supply of services to The Institute
c) The Institute is committed to providing training to all users of new systems to ensure that their use is both efficient and does not compromise information security

d) Constant training in the latest threats and information security techniques is to be prioritised to educate and train the information technology personnel.

21. BREACH OR VIOLATION OF INFORMATION SECURITY

Any failure and/or refusal to comply with the provisions of this policy will result in disciplinary action which may include dismissal or liability for damages.

22. REVIEW OF THIS POLICY

Regular review and amendments of this policy will be done in line with the approved institutional policies. This will take place in consultation with the relevant quality assurance structures at departmental and institutional level, under the auspices of the official custodians of this policy, namely the Head of Information and Technology.