NUST ICT ACCEPTABLE USE POLICY AND PROCEDURES

ICTS Department

Approved July 2018

Table of Contents

NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

ICT ACCEPTABLE USE POLICY AND PROCEDURES

1 BACKGROUND

This document constitutes a university-wide policy intended to allow for the proper use of all National University of Science and Technology (NUST) computing and network resources, effective protection of individual users, equitable access, and proper management of those resources. This document should be broadly interpreted. This policy applies to users of the NUST network and any other NUST ICT resources. These guidelines are intended to supplement, not replace, all existing laws, regulations, agreements, and contracts that currently apply to computing and networking services at NUST and Zimbabwe.

The policy is designed in compliance with the National ICT policy.

The policy seeks to protect, and apply safe and best practices.

Campus units that operate their own computers or networks are encouraged to add, with the approval of the unit head, individual guidelines that supplement, but do not lessen the intent of this policy. In such cases, the unit will inform users and provide a copy of the unit-level policy to the office of communication upon implementation.

Access to the NUST Network is a privilege, not a right. Access to networks and computer systems owned or operated by NUST requires certain user responsibilities and obligations and is subject to University policies and local and international laws. Appropriate use should always be legal and ethical. Users should reflect academic honesty, mirror community standards, and show consideration and restraint in the consumption of shared resources. Users should also demonstrate respect for intellectual property; ownership of data; system security mechanisms; and individual rights to privacy and to freedom from intimidation, harassment, and annoyance. Appropriate use of computing and networking resources includes instruction; independent study; authorized research; independent research; communications; and official work of NUST units, recognized student and campus organizations, and agencies of the University.

2 POLICY STATEMENT

2.1 Information & Communication Technology (ICT) is provided to support the teaching, learning, research and administrative activities of the University. The data held on the network forms part of its critical assets and is subject to security breaches that may compromise confidential information and expose the University to losses and other legal risks.

2.2 University guidelines and policies change from time to time, therefore users are encouraged to refer to online versions of this and other University policies on the University website.

2.3 Any infringement of these regulations may be subject to penalties under civil or criminal law, and as such law may be invoked by the University. Any infringement of these regulations constitutes a disciplinary offence under the University procedures and may be treated as such regardless of legal proceedings. Abuse of the regulations may result in the user's account(s) being suspended.

2.4 These regulations are periodically reviewed by the ICT Senate Committee for the University Senate.

3 PURPOSE

3.1 This policy has been established to:

3.1.1 Provide guidelines for the conditions of acceptance and the appropriate use of the computing and networking resources provided for the use by academic, professional and support staff and students of the University in support of the mission of the University.

3.1.2 Provide mechanisms for responding to external complaints about actual or perceived abuses originating from the University network and computer systems.

3.1.3 To provide the mechanism for responding to internal complaints about actual or perceived abuses against University systems from the internet.

3.1.4 Protect the privacy and integrity of data stored on the University network.

3.1.5 Mitigate the risks and losses from security threats to computer and network resources such as virus attacks and compromises of network systems.

3.1.6 Reduce interruptions and ensure a high availability of an efficient network essential for sustaining the businesses of the University.

3.1.7 Encourage users to understand their own responsibility for protecting the University network.

3.1.8 To ensure compliance without limitation to statutes and regulatory

4 AUDIENCE

4.1 This policy applies to:

4.1.1 Authorized users (academic, professional, support staff, students and others to whom access privileges have been extended) using either personal or University provided equipment connected locally or remotely to the network of the university.

4.1.2 All ICT equipment connected (locally or remotely) to University servers.

4.1.3 ICT Systems owned by and/or administered by the ICTS department of the University

4.1.4 All devices connected to the University network irrespective of ownership

4.1.5 Connections made to external networks through the University network.

4.1.6 All external entities that have an executed contractual agreement with the University

5 INDIVIDUAL PRIVILEGES

i) The following individual privileges, all of which currently exist at NUST, empower all members of the NUST community to be able to work towards fulfilment of the NUST vision and objectives. It must be understood that these privileges are conditioned upon acceptance of the accompanying responsibilities within the guidelines of the ICT Acceptable Use and Procedures Policy.

ii External users should note that NUST Internet access is not for free. For external users attending conferences or functions at NUST, the cost for ICT resources access should be incorporated in fees for hiring and accessing the venue.

5.1 Privacy

To the greatest extent possible in a public setting, NUST seeks to preserve individual privacy. Electronic and other technological methods must not be used to infringe upon privacy. However, NUST computer systems and networks are public and subject to the NUST ICT Acceptable Use Policy and Procedures usage Policy. All content residing on University systems is subject to inspection, and any such inspection should be carried out in the presence of the user. If the user is not available other means may be used as in Section 11.

5.2 Ownership

5.2.1 The electronic resources of the University are to be used for academic, research, consultancy or other business purposes in serving the interests of the University and its students, staff and clients and in the course of normal operations.

5.2.2 Intellectual property works created using NUST ICT resources will belong to NUST unless declared with the NUST intellectual property office in conjunction with ICTS

5.2.3 Any ICT or electronic communications address, site, number, account or other identifier associated with the University, or assigned by the University to individuals, units or functions of the University, is the property of the University.

5.2.4 Electronic communications records pertaining to the business of the University are considered University records whether or not the University owns the electronic communications facilities, systems or services used to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, print or otherwise record.

6 RESPONSIBILITIES

6.1 Council

Council has ultimate responsibility for information security within the University. More specifically, it is responsible for ensuring that the University complies with relevant external requirements, including legislation.

6.2 Senate

Senate or any future equivalent body is responsible to Council for:

a. Responsibility to source and make available resources,

b. Funding for the Senate ICT sub-committee and ICTS to implement,

c. Have oversight of policy and make available resources for the implementation of the policy.

6.3 Senate ICT sub-committee (SICT)

The Senate ICT sub-committee (SICT), or any future equivalent body, is responsible to Council for:

I. ensuring that users are aware of this and all other policies relating to the use of ICT resources at NUST;
II. seeking adequate resources for its implementation;
III. monitoring compliance of this and other policies;
IV. conducting regular reviews of the policy, having regard to any relevant changes in legislation, organisational policies and contractual obligations; and
V. ensuring there is clear direction and visible management support for security initiatives.

6.4 Vice Chancellor

a. Vice Chancellor as Chief Executive Officer for the institution is responsible for the overall information security within the whole University .
b. Overseer for the Senate ICT sub-committee and ICTS as a department to implement policy as well as avail resources for the implementation of the policy.
c. Pro-Vice Chancellors in the Vice-Chancellor’s office are responsible for the operational planning and coordination of ICT policies implementation.
d. Through the ICTS Department in the Vice-Chancellor’s office enforce all relevant policies and regulations to ensure information security

6.5 Deans / Directors

Given the University’s devolved structure, Deans are responsible for information security within their faculties. They must ensure that the faculty has in place a local information security policy to meet its own particular needs, consistent with the requirements of this overarching policy.

6.6 Heads of Departments/ Sections

Given the University's devolved structure, heads of department are responsible for information security within their departments. They must ensure that the department has in place a local information security policy to meet its own particular needs, consistent with the requirements of this overarching policy. The local information security policy should identify the department's own information security requirements and provide a management framework for meeting those requirements. 'Department' in this context includes equivalent local units, as well as divisional offices.

6.6.1 Specific roles and responsibilities for information security within departments should be clearly identified.

6.6.2 The head of department must approve the policy, and ensure that it is disseminated , implemented and regularly reviewed.

6.7 Users and External Parties

Users of University information will be made aware of their own individual responsibilities for complying with University and departmental policies on acceptable use. Agreements with third parties involving accessing, processing, communicating or managing the University's information, or information systems, should cover all relevant security requirements, and be covered in contractual arrangements.

6.8 User Responsibilities

6.8.1 The user of a University computer account or computer system connected to the University is responsible for the actions associated with the computer account or computer system.

6.8.2 Users must ensure that they use all reasonable means to protect their equipment and (if applicable) their account details and passwords

6.8.3 Engaging in any prohibited activities referred to in section 8 of the University Acceptable Use Policy and procedures may result in disciplinary action being taken.

6.8.4 Users are expected to assist ICT support staff with investigations into suspected violations or breaches of security ~~.~~

7 Acceptable Use and Personal Use

7.1 ACCEPTABLE USE

7.1.1 The University provides electronic communication systems and services to departments and faculties in support of its academic mission. ICTS encourages their use and makes them widely available to the University community. Nonetheless, the use of these facilities constitutes acceptance of this policy and is subject to the following limitations, necessary for the reliable operation of the electronic communication systems and services.

7.1.2 Users must comply with all applicable laws

7.1.3 The electronic resources should be used for the purpose for which they are intended

7.1.4 Users must respect the rights, privacy and property of others. Users are prohibited from looking at, copying, altering or destroying anyone else’s personal files without explicit permission (unless authorized or required to do so by law or regulation)

7.1.5 Users must adhere to the confidentiality rules governing the use of passwords and accounts, details of which must not be shared.

7.1.6 Passwords must not be disclosed to anyone even if the recipient is a member of ICTS. Temporary passwords provided by ICTS staff to users must be changed immediately following a successful login.

7.1.7 Whilst the University network is being used to access other networks, any abuses against such networks will be regarded as an unacceptable use of the University network.

7.2 Personal Use:

Users of the NUST ICTS resources are allowed to use the resources for personal use subject to the following guidelines:

7.2.1 The University network and computing resources may be used for incidental purposes provided that:

7.2.2 The purposes are of a private nature, not for financial gain and does not contravene any other staff policies

7.2.3 Such use does not cause noticeable or unavoidable cost to the University.

7.2.4 Such use does not inappropriately interfere with the official business of the University

7.2.5 Such use does not include any actions defined in Section 8 of the University ICT Acceptable Use Policy and Procedures.

8 UNACCEPTABLE USE

8.1 The University ICT facilities must not be provided to individual consumers or organizations outside the University except where such services support the mission of the University or are in commercial interest of the University and permission has been granted by ICTS.

8.2 The University adopts a policy of cooperation with copyright holders and law enforcement bodies, and may suspend or remove content published online while investigating claims from such bodies.

8.3 The University will from time to time act to suspend or remove content from websites which will jeopardize the University's reputation or brand.

8.4 Any misuse of the University network resources may be seen as a breach of University disciplinary and lead to disciplinary action.

8.5 The University network may not be used for the following activities:

8.5.1. The creation, dissemination, storage and display of obscene or pornographic material.

8.5.2. The creation, dissemination, storage and display of indecent images of children.

8.5.3. The creation, dissemination, storage and display of hate literature.

8.5.4. The creation, dissemination, storage and display of material that promote terrorism.

8.5.5. The creation, dissemination, storage and display of defamatory materials or materials likely to cause offence to others.

8.5.6. The downloading, storage and dissemination of copyright materials including software and all forms of electronic data without the permission of the holder of the copyright or under the terms of the licenses held by the University.

8.5.7. Any activities which do not conform to applicable laws and other University guidelines and policies regarding the protection of intellectual property and data. Specific emphasis is placed on the downloading and copying of both music and video files through the internet using peer-to-peer file sharing utilities such as but not limited to Limewire, Morpheus, Bit Torrent etc.

8.5.8. The deliberate interference with or gaining illegal access to user accounts and data including viewing, modifying, destroying or corrupting data belonging to other users

8.5.9. Using the network or centrally managed services for commercial work for outside bodies without explicit permission from the Director of ICTS.

8.5.10. Use of a username and password belonging to another user.

8.5.11. Attempts to crack capture passwords or decode encrypted data.

8.5.12. Intentional or reckless creation, execution, forwarding or introduction of any viruses, worms, Trojans or software code designed to damage, self replicate or hinder the performance of the University network.

8.5.13. Deliberate actions that might reduce the effectiveness of any antivirus or other ICT security management precautions installed by authorized University staff.

8.5.14. Attempts to penetrate security measures (hacking) whether or not this results in a corruption or loss of data.

8.5.15. Purposefully scanning internal or external machines in an attempt to discover or exploit known computer software or network vulnerabilities.

8.5.16. Engaging in commercial activities that are not under the auspices of the University.

8.5.17. Using computing resources (CPU, time, disk space, and bandwidth) in such a way that it causes excessive strain on the computer systems or disrupts denies or creates problem for other users.

8.5.18. Connecting any computer device to the University network unless it meets the desktop security standards established by ICTS on behalf of the University.

8.5.19. Any other use that may bring the name of the University into disrepute or expose the University to the risk of litigation.

9 PASSWORD POLICY

9.1 *Introduction*

Passwords are the primary authentication method for the University ICT resources. The combination of unique usernames and passwords ensure that only authorized individuals have access to specific information resources and ensure accountability for all changes made to system resources.

Strong passwords promote a secure computing environment

Users must be diligent in guarding against internal and external threats to University resources by adopting strong passwords and by not sharing them under any circumstances.

Users must not respond to emails or phone calls asking them to provide their username and password. Under no circumstances will the University or one of its agents require a user to disclose their password.

9.2 *Requirements for all users*

9.2.1. Passwords must be kept confidential and under no circumstances be shared.

9.2.2. The requirements for the setting of the password vary from time to time depending on the best industry practice. The following is an exemplary but not exhaustive list of the criteria that can be used for setting passwords: Username or variations of the username should not form part of the password

- Passwords must not be blank
- Passwords must contain alphanumeric characters
- Passwords must contain special characters

- Password length must not be less than 8 characters
- Password cannot be reused
- Passwords cannot be substantial parts of a previously used password.

9.2.3. Passwords must not be written down

9.2.4. Passwords must not be stored on digital media

9.2.5. Passwords must be changed periodically at intervals no longer than 3 months for staff and twelve months for students.

9.2.6. Passwords must be changed immediately if there is suspicion that the password confidentiality might have been compromised.

10 E-MAIL POLICY

10.1 *Introduction*

This Electronic mail (e-mail) security policy's purpose is to ensure that all e-mail correspondence conducted by employees of NUST, either internally or externally, is proper and in good conduct. To this end there are a few responsibilities, compliance and privacy issues that each user of the e-mail system has to adhere to.

This policy sets out the general rules for the use of NUST's e-mail systems, including electronic notice-boards hosted thereon, together with specific protocols and guidance concerning the Data Protection implications. E-mail and other electronic information systems will, in accordance with the university's Information Strategy, reduce the need for paper-based communication. The Institute makes available e-mail systems for use by its staff and students and encourages the appropriate use of e-mail as an alternative to paper based communication.

The university's e-mail systems are coordinated and managed by Information and Communication Technology Services. No other email systems (servers or clients) are recognised or supported within the University.

10.2 *Privacy, Confidentiality and Public Records Considerations*

NUST will make reasonable efforts to maintain the integrity and effective operation of its electronic mail systems, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, the University can assure neither the privacy of an individual user's use of the University's electronic mail resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored thereby.

All Official Outgoing Emails should contain user signatures and the signature MUST include the names and surname of sender, post held, NUST address and phone numbers and the sender contact numbers.The university will append all outgoing email with a disclaimer shown in Section 18.3.3 of the Appendix.

10.3 *Permissible Uses of Electronic Mail*

The use of any University resources for electronic mail must be related to University business, including academic pursuits. Incidental and occasional personal use of electronic mail may occur when such use does not generate a direct cost for the University. Any such incidental and occasional use of University electronic mail resources for personal purposes is subject to the provisions of this policy.

10.4 *Prohibited Uses of Electronic Mail*

Other prohibited uses of electronic mail include, but are not limited to:

10.4.1. Personal use that creates a direct cost for the University is prohibited.

10.4.2. The University's electronic mail resources shall not be used for personal monetary gain or for commercial purposes that are not directly related to University business.

10.4.3. Sending copies of documents in violation of copyright laws

10.4.4. Capture and "opening" of electronic mail except as required in order for authorized employees to diagnose and correct delivery problems

10.4.5. Use of electronic mail to harass or intimidate others or to interfere with the ability of others to conduct University business.

10.4.6. Use of electronic mail systems for any purpose restricted or prohibited bylaws or regulations of Zimbabwe and the University.

10.4.7. Spoofing i.e., constructing an electronic mail communication so it appears to be from someone else.

10.4.8. Snooping i.e., obtaining access to the files or electronic mail of others for the purpose of satisfying idle curiosity, with no substantial University business purpose.

10.4.9. Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorization.

10.4.10. Use of Electronic mail in creation or distribution of any offensive, or disruptive messages, including messages containing offensive comments about race, gender, age, sexual orientation, pornography, religious or political beliefs, national origin or disability.

10.5 *Cautionary notes*

The nature of e-mail is such that total confidentiality cannot be guaranteed and users should be aware of the following points about the use of e-mail:

10.5.1. Copies of e-mail may exist on a back-up copy or a remote system even after the author or recipient has deleted the message;

10.5.2. E-mail may be forwarded by any recipient without the author's consent,although it may not have been the author's intention. A forwarded message may be a modified version of the original;

10.5.3. It is possible for the author or sender of e-mail to disguise or alter their identity

10.5.4. Organizations outside the University may have different policies on e-mail. Some consider it the property of the organization, subject to examination, copying or forwarding. Be aware of this possibility when sending e-mail;

10.5.5 A reply to a personal message sent via a 'listserver' or electronic bulletin board may be inadvertently distributed to all subscribers to the list;

10.5.6 Usernames and passwords should not be disclosed to others. This could result in security breaches and other people using your e-mail account to send unauthorized messages. Suspected security breaches should be reported to ICTS at once;

10.5.7 Once a message is sent, there is no way to retrieve it. Check carefully that messages are addressed to the correct recipient(s) before sending.

11 Auditing

11.1 ICTS will endeavour to maintain privacy of e-mail. However, there may be special cases where it is essential that e-mail messages are accessed due to, for example, illness of the owner of a mailbox. In these instances, on the request of a Dean of Faculty or Head of Service and on the authorisation of the Head of ICT (or appropriate deputy), ICT may locate and make available e-mail messages for access by a nominated member of staff. The owner of the mailbox will be notified in due course.

11.2 Certain authorised members of ICTS may necessarily have access to the contents of e-mail messages in the course of system administration. Any knowledge thus obtained will not be communicated to others, unless required for system administration.

11.3 ICT reserves the right to take special actions in administering e-mail if this is essential to preserve the integrity or functionality of the systems. This may include the deletion of e-mail.

12 Retention

The University has an automatic centralised system to archive e-mails. This enables the University to track down previous e-mails in respect of correspondence that would be significant in an internal or external matter (e.g. correspondence of a contractual nature). It will also be used to provide access to information by the government of Zimbabwe.

The e-mails are simply to be stored as part of an archiving system.

The Institute may use personal data contained within e-mails for particular purposes when its purpose is set out or clearly implied by the nature of the e-mails. E-mails will be archived for a period of one year.

13 Deletion and Archiving

E-mail messages are archived along with other files in accordance with existing ICTS operational procedures so messages deleted by the user may still be held on archives. However, archiving of e-mail messages is not guaranteed so users should make their own copies of essential messages.

14 Email Monitoring

The University will not monitor electronic mail as a routine matter but it may do so to the extent permitted by law, as the University deems necessary for purposes of maintaining the integrity and effective operation of the University's electronic mail systems.

15 Security - Opening and Closing of Accounts

Computer and e-mail accounts for staff are set up by ICTS on receipt of a request from Personnel. Associated passwords are issued directly to the end user or via Faculty administration. Staff accounts are deleted on receipt of a request from Personnel. Student accounts are created automatically after enrolment of the student and remain active until the end of the course or receipt by ICTS of notification of withdrawal. Student passwords are issued in accordance with the current procedures.

Before leaving employment at NUST, staff should unsubscribe from any e-mail lists that they may have subscribed to and delete any personal e-mails in their account. If there are any work-related e-mails that need to be transferred to another email client then these e-mails should be forwarded on as appropriate - the ICTS department can be e-mailed if any assistance is required.

Following the departure of a member of staff from the University, their e-mail account will be closed and an "out of office" message set for a period of 12 weeks after which time the account will be deleted. NUST management may request access to be given to the closed mailbox by another member of staff for this duration.

16 Inspection and Disclosure of Communications

The University reserves the right to inspect and disclose the contents of electronic mail:

- in the course of an investigation triggered by indications of misconduct or misuse,
- as needed to protect health and safety,
- as needed to prevent interference with the academic mission, or
- as needed to locate substantive information required for University business that is not more readily available by some other means.

The University will inspect and disclose the contents of electronic mail when such action is necessary to respond to legal processes and to fulfil the University's obligations to third parties.

17 Compliance

Appropriate disciplinary action will be taken against individuals found to have engaged in prohibited use of the University's electronic mail resources. If any need arises to waiver policy communication should be done to the ICTS director.

Acknowledgement

NUST will take any violations of this e-mail policy or related policies like the Information Security Policy very seriously. NUST reserves the right to discipline, terminate or prosecute any user who violates any of these mentioned policies.

18 APPENDIX

18.1 DEFINITIONS

Authorized use-Authorized use of NUST-owned or operated computing and network resources is use consistent with the education, research, and service mission of the University, and consistent with this policy.

Authorized users-Authorized users are:

(1) Current Academic and Non-Academic staff, Registered Students and Current University Council members

(2) Individuals connecting to a public information service; and

(3) Others whose access furthers the mission of the University and whose usage does not interfere with other authorized users' access to resources. In addition, all users must be specifically authorized to use a particular computing or network resource by the campus unit responsible for operating the resource.

(4) External users whose registration fees or prior arrangements have been authorised for the specific duration indicated

18.2 General Email guidelines

18.2.1 Check your e-mails regularly.

18.2.2 Employees are expected to answer email with in 8 working hours of receiving an email.

18.2.3 Emails, which have cc recipients, should be replied in the same manner. i.e. The replier should also put the original cc recipient as a cc recipient in the reply.

18.2.4 Use of the bcc field: Use of bcc is encouraged if you are sending mail to a group of people where others may not want their addresses publicised. This is to protect privacy of other people's email addresses.

18.2.5 Be polite. Messages sent by e-mail can often seem abrupt, even when this is not the intention. Use professional courtesy and discretion. The use of all upper-case text in either the subject or the body of an e-mail should also be avoided as this is deemed to be the e-mail equivalent of shouting;

18.2.6 Do not reply "With History" if it is not necessary especially if it incorporates a large attachment.

18.2.7 Use 'reply all' and distribution lists with caution in order to keep the number of your messages to a minimum and reduce the risk of sending messages to the wrong people;

18.2.8 Set the Out-of-Office flag and arrange for someone to deal with your e-mail if you are away;

18.2.9 Messages should be clearly addressed to those from whom an action or response is expected, "cc" or "bcc" should be used for other recipients of the message;

18.2.10 Respect privacy and consider this aspect before forwarding messages;

18.2.11 Delete unwanted or unnecessary e-mail. It is the user's responsibility to manage their own e-mail folders and keep within the quota limits set. ICTS can give advice and assistance if required;

18.2.12 Unsolicited e-mail, especially with an attachment, may contain a virus. If in doubt, delete the e-mail or contact the sender to check before opening;

18.2.13 Do not try to carry out confidential or sensitive tasks or air controversial views on e-mail;

18.2.14 Enter a meaningful 'subject' field to help the reader anticipate the content correctly, and try to keep to one subject per message;

18.2.15 Don't use all or part of someone else's message without acknowledgement.

18.2.16 Don't edit someone else's message without making it clear the changes that you have made and don't distribute other people's messages without permission;

18.2.17 Avoid subscribing to unnecessary mailing lists. Unsubscribe from mailing.lists when they are no longer required;

18.2.18 Do not forward on e-mail "chain letters". These are e-mails which either ask you to forward them on to all your friends (or to everyone you know) or which state that something bad will happen if you do not forward them on. E-mails of this type, which are warning about something (e.g. computer viruses), are almost certainly hoaxes as well. If you are unsure about any e-mail that you've received then students can contact Computer Laboratory staff for information and staff can e-mail the ICTS staff.

18.3 *Substantive Rules*

18.3.1 Users are advised never to open mail especially containing attachments from unknown sources.

18.3.2 The following mail attachment extensions will not be allowed .exe .rar .pif. scr. The email server will block any mail outgoing or incoming containing such attachments and the administrators might add more file extensions to the list as deemed fit.

18.3.3 In addition all messages will be appended with the following disclaimer:

'This message is intended only for the named recipient . If you are notified that disclosing , copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited. This email is confidential , may be legally privileged, and is for the intended recipient only . If an addressing or transmission error has misdirected this email please notify the author by replying to this email. If you are not the intended recipient you must not use , disclose, distribute, copy, print or rely on this email. Any views or

> *opinions presented are solely those of the author and do not necessarily represent those of the National University of Science and Technology. The National University of Science and Technology, Zimbabwe, does not accept legal responsibility for the contents of this message. Whilst all reasonable steps are taken to ensure the accuracy and integrity of information and data transmitted electronically and to preserve the confidentiality thereof, no liability or responsibility whatsoever is accepted if information or data is, for whatever reason, corrupted or does not reach its intended destination. Replies to this email may be monitored by the National University of Science and Technology, Zimbabwe for operational, security or business reasons.*

18.3.4 Any user of the University's electronic mail resources who makes use of an encryption device to restrict or inhibit access to his or her electronic mail must provide access to such encrypted communications when requested to do so under appropriate University authority.