CHIETA ICT POLICY

1. *Introduction*

The policy should be interpreted in conjunction with the integrated ICT Governance Framework of CHIETA in optimal support to CHIETA stakeholders and skills development within the chemical sector.

This policy covers the integrated CHIETA IT use of information systems and technologies. This policy makes it clear that CHIETA owns and controls all workplace technology and therefore all communications and activity conducted over it. Authorised use of the CHIETA -owned or operated computing and network resources shall be consistent with the business objectives of CHIETA and consistent with this policy. Underlying this policy is the principle that each employee and business unit has a responsibility to use the CHIETA information technology resources in a manner that provides optimal service delivery to stakeholders, increases productivity, enhances the CHIETA public image, and is respectful of other employees.

Information Technology Resources Defined:

Information technology resources consist of all electronic devices, software, and means of electronic communication including, but not limited to, the following:

- Corporate Networks (LAN & WAN)
- MIS
- Servers
- Pastel
- VIP
- Notebooks and Workstations
- Fax machines & Copiers
- Telephones and associated Voice mail Facilities
- computer software applications and associated files and data, including software that grants access to external services, such as the Internet; electronic mail; telephones; cellular phones; 3G; and voicemail systems.

2. *Objectives and Critical Success Factors*

The objective of the policy is to contribute to a holistic integrated ICT Framework that embeds ICT Corporate Governance as a subject of governance within CHIETA and the creation of business value through ICT enablement by ensuring strategic business and ICT strategy alignment.

Due to the rapidly changing nature of information technology it is increasingly important that the use of all information technology systems be consistent with best practice to ensure optimal stakeholder value by employees and service providers as per the CHIETA ICT Management Framework and in direct support of deliverable defined in the CHIETA Strategic Plan.

Where this policy cannot cover specific circumstances and technologies, “acceptable use” will be based on the legal obligations of employees, the CHIETA’s code of conduct and value systems, strategic programmes as defined in the CHIETA Strategic Plan and ICT Governance Framework.

The policy also impacts on many aspects of the employee / employer relationship and should be interpreted in the context of the CHIETA staff employment policies.

CHIETA will provide support to end users in the effective use of ICT systems and in the interpretation of this policy to continuously ensure a common mind-set on roles, accountability and performance standards as defined in the ICT Charter and in direct support to the attainment of CHIETA strategic objectives.

3. *Expectation of ICT Function: Strategic Leadership*

Roles, structure and accountability level from the Accounting Authority (Governing Board) to the ICT Business Unit is clearly defined within the CHIETA ICT Governance Charter.

Compliance with these structures and processes is key in support of the ICT strategic planning processes of CHIETA and subsequent monitoring, evaluation and reporting within the collective organisational and governance levels of CHIETA to enable value-adding positioning and functions of IT as an integral part of the strategic business agenda of CHIETA.

Monitoring and reporting on ICT service delivery and performance will be reported via the ICT unit and various ICT project owners through the ICT Steering Committee, MANCO and CHIETA Governance Structures.

It will be the role of the ICT Unit and ICT Governance Champion specifically to monitor with the assistance of business units the performance of ICT based projects / programmes, conformance to the ICT governance context, laws, regulations and performance of ICT service providers which include ICT Business Continuity, ICT security management and ICT risk management.

4. *ICT Planning Process*

All CHIETA projects need to be contextualised and defined in terms of the relevant ICT support / requirements needed to ensure successful execution and attainment of project deliverables. This will form part of the annual strategic planning process of CHIETA and will be a core theme in the IT Strategic Plan.

The ICT perspective must form part of each project proposal / scoping through defining ICT support / platform needed, costs involved and ICT risks associated with each project, which will be included and presented as part of the annual ICT Management Framework.

These projects need to be conceptualized by relevant Business Units as part of the strategic planning process with the ICT perspective presented at the CHIETA ICT Steering Committee for presentation to MANCO and subsequent recommendation to the Accounting Authority (Governing Board) where relevant.

5. *Internal and External Stakeholders*

Internal and external stakeholders are defined clearly within the ICT Governance Charter. The organisational logic is enabling ICT solutions that are core and value adding to the strategic delivery and objectives of CHIETA.

Through the ICT Framework, internal stakeholders (staff) will be made aware and capacitated to deliver service standards to CHIETA stakeholders in a sustained and value adding manner.

6. *CHIETA Prescriptive Landscape*

The CHIETA prescriptive landscape is clearly defined in the CHIETA Strategic Plan mandated by the CHIETA Accounting Authority (Governing Board).

7. *Compliance and Role of ICT Function*

The role of the ICT unit is clearly defined in the ICT Governance Charter and also defines the holistic ICT Governance structure of CHIETA.

8. *Information Secrecy and Privacy*

CHIETA does not distinguish between the use of electronic media from any other media in implementing secrecy, confidentiality, copyright or other information policy.

All information originated, recorded, stored and transmitted using the organisation’s information systems is regarded as organisation property unless this is subject to copyright or third party licence agreements.

Information stored on the organisation’s systems is subject to inspection or monitoring (by the organisation) to ensure compliance with policy. By making use of the organisation’s electronic systems (which are provided for legitimate business purposes), end users acknowledge the organisation’s right to access any information held therein.

Use of the organisation’s systems for reproduction of copyright material is subject to legally accepted principles governing copyright.

Use of the organisation’s systems to reproduce or transmit trademarks, trade names or trading styles are protected by statute and end users are required to adhere to current legislation in the use of the systems.

End users are responsible for ensuring that any information of a secret, sensitive or valuable nature is transmitted in a secure manner through the organisation’s systems.

Techniques to protect sensitive information include certificates, digital signatures, encryption, password protection or physical protection.

The digital certification of electronic content by a third party certification authority or local registration authority is subject to authorisation by the CEO through the IT Manager, who will ensure that such initiatives are co-ordinated across the organisation.

9. Change Management Process

CHIETA follows a detailed program change process. Please refer to the Change Management process procedure document available on the server.

10. ICT Security

Generally, employees are given access to the CHIETA's various technologies based on their job functions.

For a detailed explanation of the CHIETA ICT Security please refer to the approved CHIETA ICT Security Policy available on the server.

Identification of Security Compromises:

The CHIETA will implement Group policies to ensure that relevant Microsoft Security Updates and Microsoft hot-fixes are promptly identified and installed, to reduce the risk of the systems being compromised, damaged or exploited.. For a detailed understanding please refer to the CHIETA Patch Management Procedure.

11. Access to Information Technology Resources

Approval of the access request:

- ➢ All users that require access to CHIETA ICT resources will be required to complete the necessary application form and have the applications form authorised by his line manager/supervisor/director.
- ➢ No access will be granted without the said authorised application.

Resetting of passwords:

- ➢ Password reset requests will be done in writing to CHIETA ICT, and the individual will have to provide proof that he is the owner of the user name and password before a password reset will be done.

Modifications to access rights (users transferred):

- ➢ Modifications to access rights will be done in line with the Change Control procedures of CHIETA, and CHIETA ICT will verify the change with the requestor's line manager/supervisor/director before the access modification will be executed.

Monitoring actions of system controllers on application security level (Creation of ID, user ID maintenance,

allocating functions to users):

Access logs pertaining to the administrative actions performed on user account management will be reviewed by CHIETA management and compared to the authorised requests to ensure that no untoward actions were taken with regards to user account management. **Sharing of Access:**

- Computer accounts, passwords, and other types of authorisation are assigned to individual users and must not be shared with others. The user is responsible for any use of the users account. If an account is shared or the password divulged, the holder of the account will lose all account privileges and be held personally responsible for any actions that arise from the misuse of the account.

Permitting Unauthorised Access:

- Users may not run or otherwise configure software or hardware to intentionally allow access by unauthorised users.

Circumventing Security:

- Users are prohibited from attempting to circumvent or subvert any system's security measures. Users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

Breaching Security:

- Deliberate attempts to degrade the performance of the Information system or network or to deprive authorised personnel of resources or access to any of the CHIETA computer or network is prohibited. Breaches of security include, but are not limited to, the following: creating or propagating viruses, hacking, and password grabbing.

12. *Management Access to Technology Resources*

Information is CHIETA Property:

All messages sent and received, including personal messages, and all data and information stored on the CHIETA's electronic mail system or Information systems are CHIETA property regardless of the content. As such, the CHIETA reserves the right to access all of its information technology resources including its computers, and electronic mail systems, at any time, at its sole discretion.

Employee Privacy:

Although the CHIETA does not wish to examine personal information of its employees, on occasion, the CHIETA may need to access its information technology resources including computer files and electronic mail messages. Employees should understand, therefore, that they have no right of privacy with respect to any messages or information created or maintained on the CHIETA's Information technology resources, including personal information or messages.

The CHIETA may, at its discretion, inspect all files or messages on its information technology resources at any time for any reason. The CHIETA may also monitor its information technology resources at any time in order to determine compliance with these policies, for purposes of legal proceedings, to investigate misconduct, to locate information, or for any other business purpose.

Employees should assume that any communication - whether business related or personal that they create, send, receive, or store on the CHIETA’s Information Technology resources may be read or heard by someone other than the intended recipient. In particular, highly confidential or sensitive information should not be sent through e-mail, the Internet, or the World Wide Web.

The CHIETA reserves the right to keep an employee's e-mail address active for a reasonable period of time following an employee's departure from the CHIETA to ensure that important business communications reach the CHIETA.

Monitoring:

The CHIETA has the right to monitor any and all usage of its Information Technology systems including (but not limited to) sites visited by users on the Internet, chat groups, and newsgroups, and downloaded or uploaded of software. All employees must be aware that the CHIETA may use automated software to monitor documents created, stored, sent, or received.

Passwords:

Some of the CHIETA's information technology resources can be accessed only by entering a password. Passwords are intended to prevent unauthorised access to information. Passwords do not confer any right of privacy upon any employee of the CHIETA. Thus, even though employees may maintain passwords for accessing Information Technology resources, employees must not expect that any information maintained on the Information Technology resources, including electronic mail are private. Employees are expected to maintain their passwords as confidential. Employees must not share passwords and must not access co-workers' systems without express authorisation.

Data Collection by the CHIETA:

The best way to guarantee the privacy of personal information is not to store or transmit it on the CHIETA's information technology resources. To ensure that employees understand the extent to which information is collected and stored, examples of information maintained by the CHIETA are given below. The CHIETA may, however, at its sole discretion, and at any time, alter the amount and type of information that it retains.

- **Electronic Mail:** Electronic mail is backed up. Although electronic mail is password protected, an authorised administrator can reset the password and read electronic mail.

- **Internet Use:** Internet usage is monitored by a firewall with pre-set settings which block the high risk content and material as listed in the policy. Firewall log reports are also monitored and reviewed..

- **Deleted Information:** Deleting or erasing information, documents, or messages maintained on the CHIETA's Information Technology resources is, in most cases, ineffective. All employees should understand that any information kept on the information technology resources may be electronically recovered regardless of whether it may have been "deleted" or "erased" by an employee. Because the CHIETA periodically backs up all files and messages, and because of the way in which Workstations and Notebooks re-use file storage space, files and messages may exist that are thought to have been deleted or erased. Therefore, employees who delete or erase information or messages should not assume that such information or messages are confidential.

13. *Abuse of Information Technology Resources*

Abuse of the CHIETA computer resources is prohibited and includes, but is not limited to:

Illegal Activity:

An employee cannot use the CHIETA's Information system facilities to knowingly break any laws and regulations of the country. Use of the Internet for illegal purposes will be grounds for termination of the employment relationship.

Game Playing:

Information system and network services are not to be used for recreational game playing. Game playing on CHIETA time is counterproductive.

Chain Letters:

The propagation of chain letters is considered an unacceptable practice by the CHIETA and is prohibited. If a chain letter is received by an employee, the CHIETA prohibits the forwarding of the email to anyone.

Faxing:

Using the CHIETA fax machine or computer faxing capabilities for non-CHIETA related activities is strictly prohibited. The CHIETA prohibits the use of any telephone facsimile machine, computer, or other device to send an unsolicited advertisement to a telephone facsimile machine unless authorised by management.

Harassing, Discriminatory, and Defamatory use:

Employees use electronic mail for correspondence that is less formal than written memoranda. Employees must take care, however, not to let informality degenerate into improper use. The CHIETA does not tolerate discrimination or harassment based on gender, pregnancy, childbirth (or related medical conditions), race, colour, religion, national origin, ancestry, age, physical disability, mental disability, medical condition, marital status, sexual orientation, family care or medical leave status, or any other status protected by the laws of the country. Under no circumstances may employees use the CHIETA's information technology resources to transmit, receive, or store any information that is discriminatory, harassing, or defamatory in any way (e.g., sexually explicit or racial messages, jokes, cartoons).

Gambling:

The use of CHIETA's Information system and networks to gamble is strictly prohibited.

Online Shopping:

The use of the CHIETA's Information system and the Internet to conduct personal online shopping is prohibited.

Unauthorised Monitoring:

A user may not use computing resources for unauthorised monitoring of electronic communications. However, the CHIETA has the right, but not the duty, to monitor any aspects of its Information system including monitoring sites visited by employees, chat groups, newsgroups, and downloading and uploading of files.

Flooding or Spamming:

Posting a message to multiple list servers or news groups with the intention of reaching as many users as possible is prohibited. Spamming email addresses within or outside the CHIETA is also prohibited.

Private Commercial Purposes:

The Information system resources of the CHIETA shall not be used for personal or private commercial purposes or for financial gain.

Political Advertising and Campaigning:

The use of the CHIETA Information system and networks shall not be used for political purposes.

Software Piracy:

Access to the Internet enables users to download a wide variety of software products for a fee as shareware or for free. The user is required to fulfil all license and copyright obligations of software that he/she download for their own use. These software downloads become the property of the CHIETA. Any employee who knowingly violates this software piracy rule is subject to termination.

Approved Software:

The following is a list of approved software, the CHIETA reserves the right to remove any software applications that are not listed below, should a user want to download or load any other application on their workstations and notebooks this must be requested by e-mail to the IT department and approved by the company.

- Microsoft Windows Operating System
- Microsoft Office Professional
- Adobe Acrobat Reader (latest release)
- Adobe Acrobat Creator
- Any other Microsoft application that is considered a work tool and that is licensed.
- 3G software that is provided by an Internet Service Provider
- VIP and Pastel (latest versions)
- Business Banking software

Unapproved software:

The following is a list of software that is not approved for use on CHIETA’s notebooks or workstations and should under no circumstances be downloaded or loaded by media:

- Any peer to peer music and or video download application such as Limewire or Torrentz
- Games, or otherwise any application not approved by CHIETA as approve software

Use of Unlicensed Software:

The use of unlicensed software on CHIETA’s workstations and Notebooks are strictly prohibited. All software in use on the CHIETA's information technology resources must be officially licensed software. No software is to be installed or used that has not been duly paid for and licensed appropriately for the use to which it is being put. No employee may load any software on the CHIETA's workstations or notebook, by any means of transmission, unless authorised in writing in advance by the Administration Division Head and the IT Manager. Authorisation for loading software onto the CHIETA's computers will not be given until the software to be loaded has been thoroughly tested for compatibility with the Information system and has been scanned for viruses.

Software for Home Use:

Although some software licenses allow software to be used on notebooks and home computers in addition to office workstations, before transferring or copying any software from a CHIETA Information Technology resource to another computer, employees must request permission and receive written authorisation. Authorisation should be obtained from the Executive Manager of a particular business unit with advice/recommendations from the IT department.

Pornography:

Employees are not allowed to visit sites that are considered “obscene”. The CHIETA may maintain a system to monitor Internet usage. In the event that an employee disregards this policy and continually visits “unauthorised” sites, it will be grounds for termination after a warning has been issued to the employee. The CHIETA has the right to view private files that have been downloaded to check for the propriety of these downloads. The CHIETA also prohibits using CHIETA Information Technology resources to send sexually oriented images or messages.

14. E-mail Policies

Acceptable e-mail Usage:

Personal use of the organisation’s e-mail is permitted, within reason, however the organisation reserves the right to intercept & monitor such communications to ensure compliance with this policy.
Personal use of the organisation’s systems for e-mail is permitted providing that it does not consume significant time, or band width, or adversely affect employee productivity and affect the efficiency of systems (large attachments).

The following material may not be transmitted or retained on the organisation’s email systems:

- Obscene, defamatory or discriminatory material
- Sexually explicit messages
- Religious or racial slurs
- Infringement of another person's intellectual rights
- Insulting, disruptive, offensive, or other material harming the organisation's morale
- Material violating the terms of laws governing cross border data flow

E-mail Passwords:

Only authorised employees issued e-mail passwords are permitted to use passwords to access their own e-mail accounts. Only authorised employees are permitted to use the password of another employee to access that employee's e-mail account. Misuse of passwords and the unauthorised sharing of passwords will result in disciplinary action.

Junk Mail and Spamming:

Use of the organisation's mail systems shall be for legitimate business purposes and limited private use. The transmission of "junk mail", private or unsolicited advertising is not permitted.

Attachment size:

Sending of e-mails with large attachments may impact adversely on the infrastructure and may be limited from time to time by the I T department. Such limitations shall take into consideration the load on the systems, the need for such attachments for work purposes and the possibility of delaying the sending of such mail until off-peak periods.

E-mail storage space:

Limits may be set from time to time on the storage space occupied by each end user. This limit will be determined by the storage capacity of the mail server. Users are advised to move important documents into public folders made available on the mail server and not keep copies in their personal mailboxes.
The capacity of Inboxes is monitored and users will be prompted to clear their inboxes when capacity approaches.

Forwarding e-mails:

Users may not forward e-mail to others without the express permission of the sender. The express permission is necessary since frequently e-mail contains confidential, proprietary, and trade secrets. All employees must consider that e-mail messages meant for a single reader may not be meant for widespread distribution.

Chain Letters:

Employees are prohibited from initiating or forwarding chain letters via e-mail. A chain letter is a message sent to a number of people asking each recipient to send copies with the same request to a specified number of others.

Bulk Email:

In general, the use of the CHIETA's email system as medium for the bulk distribution of information is discouraged.

On rare occasions, email may be the best mechanism to distribute information to large segments of the CHIETA community. Approval from the IT department is required for messages sent to more than 30 people.

In addition, these guidelines should be followed:

Messages should be plain text with no attachments. (If recipients require another kind of material, it can be posted at a website and links can be included in the message.)

Distribution lists should be kept private. This can be done by listing recipients in Bcc: addresses instead of To: addresses or Cc: addresses.

Timing and other details of bulk mailings should be coordinated with the IT Manage and Administration Division Head.

Accurate Communication via e-mail:

All employees should make every attempt to communicate truthfully, accurately, and clearly via e-mail. Employees should use the same due care in drafting e-mail as they would for any other CHIETA communication.

E-mail manners:

Generally e-mail is “abused” more through ignorance than intent. There are a few “don’ts” which are universally understood as bad practice and are not permitted on the CHIETA information systems. In particular:

- Forwarding “chain letters” through the organisation’s e-mail system
- Forwarding virus warnings to the whole organisation. Rather send it to the IT Manager who will communicate appropriately
- “Shouting” – THE PRACTICE OF USING UPPER CASE TO MAKE A POINT
- Sending large attachments to a large mailing list. For example a 1Mb message with 3 image attachments sent to 40 people, could occupy 120Mb of server hard disc space and countless backup capacity and severely clog up the organisation’s links. Recipients should delete these messages as soon as possible
- Personal or commercial advertisements sent to a large distribution list. This is known a “spam”
- “Flaming” – the practice of destructive debate or argument in public by virtue of e-mail distribution lists
- The practice of setting the “Urgent” flag by default. People eventually respond by setting a mental rule to ignore certain users who use the “cry wolf” syndrome

- Using inappropriate distribution lists. Don’t send an e-mail to someone unless it truly affects that person. Equally, don’t reply to every message by default. Think first!
- Hiding behind e-mail to communicate unpopular issues or delegating tasks that are better communicated personally

Formatting:

The following practices are to be adopted by all staff:

- The organisation’s language is English (South Africa)
- E-mail font is Arial 10, Regular, Black, Western Script
- Background is White
- Measurement system is “metric”
- Date protocol is dd/mm/yy
- Hot bars occupy unnecessary disk space and should be removed from screens

Spoofing:

Employees are prohibited from hiding their identity (spoofing) when sending e-mail. Any anonymous or pseudonymous e-mail messages are prohibited.

15. *Communication of Confidential and Sensitive Information via e-mail*

Sending via e-mail proprietary information, trade secrets, or other confidential information of the CHIETA is strictly prohibited. This type of information is a valuable asset of the CHIETA. Unauthorised dissemination of this type of information may result in civil liability as well as criminal penalties. E-mail messages are like paper documents. Client-related e-mail messages should be carefully guarded and protected. Before sending an e-mail message, every employee should think about how a third party to the message might interpret the message.

Blind ‘Carbon Copies’:

Due care must be exercised when sending blind carbon copies (blind cc) of e-mail messages. All employers using “blind cc” must ensure that the addressee’s privacy is not violated.

E-mail Ownership Policy:

All e-mail messages the user create, receive, and use in the course of business is the property of the CHIETA. It does not belong to the user or other employees or to any third party. At management's request, employees must make available any or all CHIETA records (including e-mails). The law gives the management of the CHIETA the right of access to all employee messages sent or received via CHIETA systems. With regards to e-mail, employees have no expectation of privacy.

E-mail Retention:

E-mail is a generic term and does not refer to any particular type of record however, most e-mail is typically considered correspondence. Records in e-mail systems include not only the messages sent and received, but also the transmission and receipt data as well.

Since e-mail is considered a type of correspondence, e-mail retention periods should agree with CHIETA records retention policy. If you have determined that the e-mail message is not correspondence, but it is another type of record, then review the appropriate retention schedule to determine the applicable retention / disposition period.

Certain e-mail messages may be considered non-records and these may be kept in personal folders. Examples of such non-records include:

➢ Non-business messages

➢ Courtesy copies (duplicates) of messages.

➢ Minor, non-policy announcements, or reminders, i.e., CHIETA social functions, etc

All employees are responsible for retaining e-mails. Employees are also responsible for deleting drafts and non-business e-mail messages once they are no longer needed. Do not assume that even though the user has deleted e-mail messages that they cannot be recovered.

Subscriptions to mail list:

End users are advised against subscribing to mailing lists with their organisation e-mail address, unless these have a specific business purpose. Users are responsible for maintaining subscription details and unsubscribe when information is no longer required.

16. *Spyware Policy*

The CHIETA Workstations and Notebooks often contain private information. Unapproved software or hardware that monitors web browsing, keyboard use or related activities must not be installed on the CHIETA Workstations and Notebooks. Software installed on the CHIETA Workstations and Notebooks must be selected cautiously. Some prohibited spyware is distributed as "free" software, for which consumers agree to allow their activities to be monitored in exchange for use of the software.

Use of spyware on personally owned computers connected to the CHIETA network is prohibited. Use of programs to detect and expunge spyware is encouraged on all computers connected to the CHIETA network.

This restriction is not intended to limit in any way the CHIETA's right to monitor any and all hardware or software owned by the CHIETA, or connected to the CHIETA network, for the purposes of preventing or investigating improper or illegal use of the CHIETA systems, or preventing or investigating system problems or efficiencies.

17. Internet Usage Policy

The CHIETA has made substantial investments to make it possible for the end user to electronically communicate with fellow employees and customers as well as to seek information from the worldwide web. The purpose of these investments is to help the end user/employees do their job in a more efficient manner. The CHIETA's facilities that make this possible include costs for telecommunications, networking, additional software, and mass storage. This policy is designed to define expectations for what is acceptable and what is not when it comes to using these resources wisely.

To reiterate, Internet usage at the CHIETA is provided to the user because of a significant investment and it is expected that the user use these resources for business purposes. Examples of appropriate usage include the following:

- Researching topics that are relevant to the user's specific job requirements.
- Communicating with fellow employees, customers, prospects, and suppliers.

Under no circumstances are employees permitted to use the Internet to access, download, or contribute to the following:

Gross, indecent, or sexually oriented materials
Sports sites
Job search sites
Entertainment sites
Gambling sites
Games, humour
Illegal drug oriented sites
Personal pages of individuals
Politically oriented sites

Confidentiality and the Internet:

Issues of confidentiality take on critical importance when it comes to the Internet. The Internet provides a new level of communication enabling all levels of CHIETA employees to make statements on behalf of the CHIETA. When a CHIETA employee sends a message or communicates through a public forum as an employee, it is natural for the recipient of that message or communication to understand it to be a CHIETA position or message. In fact, as will often be the case, it may just be a personal opinion.

Under no circumstances should employees disseminate CHIETA confidential information over the Internet to anyone that is not covered by a Non-Disclosure Agreement (NDA). Great care must be taken even when sending confidential information to individuals who are covered by NDAs (Non-Disclosure Agreements). It is very easy to make a mistake when messages are sent to inadvertently include wrong addresses or the wrong file for that matter. Security and confidentiality need to be extremely high concerns for all CHIETA employees.

When confidential files are sent over the Internet, users must take great care in disseminating them. It is strongly recommended that files be encrypted before file transmissions.

Sexual Harassment:

Displaying sexually explicit images on CHIETA property is a violation of the CHIETA policy and code of conduct. The employee is not allowed to download, archive, edit, or manipulate sexually explicit material while using CHIETA resources. If an employee receives material from the outside that is sexually explicit, it is wise to destroy it and advise the sender of the material that you do not wish to receive any additional material of this nature. If the originator of this material is another CHIETA employee, you should warn the employee of the CHIETA policy about sexual harassment. If the employee persists in sending the material, the incident should reported to the individual's line manager and to the Human Resource Manager.

Public Forums:

Employees are allowed to enter public forums when it makes business sense to do so. Only those employees that are authorised to speak on behalf of the CHIETA may do so in the name of the CHIETA in any newsgroup, public forum, or chat rooms. Employees that do not have this authorisation cannot make statements as an individual on behalf of the CHIETA. Therefore it is necessary to identify yourself as an individual (not as a CHIETA spokesperson) when you enter any public forum. If asked whether your comments can be construed as a CHIETA statement, you can only make this claim if you are an authorised person to do so. All confidentiality matters apply to public forums. It is important to reiterate that you should make no comments about CHIETA confidential information.

Guest Books, Newsgroups, and Bulletin Boards:

Additionally, employees must not sign "guest books" at Web sites or post messages to Internet news groups or discussion groups at Web sites. These actions will generate junk electronic mail and may expose the CHIETA to liability or unwanted attention because of comments that employees may make. The CHIETA strongly encourages employees who wish to access the Internet for non-work related activities to obtain their own personal Internet access accounts. Employees may subscribe to newsgroups providing they involve work-related topics such as local events, groups, or educational issues, however, even the use of those information resources via the CHIETA's information technology resources must be approved by management.

Private Internet Use:

If you use the Internet at home on your own account, your privileges and privacy are assured. However, all confidentiality clauses remain – i.e., you may not make statements as a CHIETA employee. You can represent yourself as a CHIETA employee but make sure that your comments are your personal opinion. In all cases refrain from making statements or opinions that could affect the CHIETA's confidentiality or image.

18. *Content Filtering*

The general policy of the CHIETA is to avoid filtering content passed through the CHIETA network. However, content filtering may occur in the following circumstances:

- The CHIETA will filter network traffic if it is legally required to do so.
- The CHIETA may block e-mail from sites known to send or transport excessive amounts of unsolicited bulk e-mail.
- The CHIETA may scan e-mail for viruses, worms and other malicious programs. E-mail containing such programs may be refused either in whole or in part.
- The CHIETA may block traffic likely to compromise the privacy of the CHIETA information or the security and integrity of either internal or external networks.
- The CHIETA may prioritise traffic passing through its network based on assumptions about traffic types and their requirements for quality of service.
- The CHIETA may block messages and attachments deemed to be too large.

19. *Internet Access and Administration*

The CHIETA reserves the right to limit access to the Internet for those employees who are required to use it.

The CHIETA also reserves the right to monitor the usage of the Internet. This includes the following:

- The blocking of certain sites that have been deemed offensive. Trying to subvert this blocking will be grounds for termination.
- Monitoring the usage rates of the Internet by all employees and individual usage. The CHIETA reserves the right to publish this information on an internal basis.
- Monitoring the specific sites that each employee visits, and the length of each visit.
- All file transfers and e-mail deliveries will be monitored.
- None of the users communications and Internet visits made during business hours are considered private therefore, treat all of the users activities as such. The CHIETA reserves the right to inspect files and communications that the user makes to assure compliance with this policy.

Making CHIETA Purchases over the Internet:

Employees who have budgetary approval may use their company credit cards to purchase products for CHIETA use over the Internet. Before doing so however, confirmation must be obtained with the IT department first regarding the safety and security of the website.

Virus, Trojan Horses, etc.:

All files that are downloaded must be first scanned for possible infection. Any employee who knowingly tries to propagate the Internet or internal resources with infected viruses or Trojan Horses will be liable for misconduct.

20. *Third party access*

Any third party (contractor, agent, family member etc.) may only access the organisation's information system if such person has entered into a non-disclosure or secrecy agreement.
Third party users of the organisation's systems must be made aware of, and operate within the parameters of this policy.

21. *Offsite access to organisation information*

The CHIETA will provide access to the organisations systems from offsite locations to authorised users. The remote location should be seen as an extension of the office environment with the additional risks of physical security, shared computing resources, unauthorised access and increased data transmission through the public infrastructure.
Access to the organisation's systems from a remote location through dial up or web access is subject to all the provisions of this policy. Dial up users should be aware of their obligations under this policy and ensure that appropriate measures are taken to minimise these risks.

Best practices include:

- Securing the offsite computer physically to prevent loss by theft or unauthorised access
- Limiting the work related content on the remote computer to essential files only
- Password protecting the remote computer and data
- Ensuring that the remote computer is not connected to the organisation's systems without the designated end user present
- See also the best practices applicable to notebooks and portable devices below

22. *Use of organisation's Notebooks and other portable devices*

Organisation information stored on notebooks and portable devices should be protected against unauthorised access from e.g. theft.
Best practices include:

- Using a secure operating system (Windows NT, 2000, Vista and Windows 7) with NTFS file partition
- Password protecting access to work-related files on the notebook
- Password protecting access to the offline mail store if this exists
- Never saving passwords to the portable device

- Limiting the amount of documentation that is carried on a portable device to essential material only.

  The end-user remains responsible for the secure operation of portable devices when offsite.

Allocation of Notebooks and other portable devices:

Notebooks will be allocated and approve by the CEO taking consideration the employees job profile and responsibly areas.
Floating' notebooks will be kept in the IT department and managed as part of the CHIETA Asset Management Framework.

23. Storage of organisation data

Shared folders on the network will be made available for the storage of department or individual information. End-users should make use of these facilities and avoid storing business information on local hard drives or portable devices.
No back-ups are made of local drives and end users are responsible to ensure that loss of such a device does not result in loss of organisation information.

24. Unlicensed Software

The following will not be allowed with regards to software with regards to the CHIETA ICT infrastructure:

- Software that is not licensed;
- Software that threatens the security of CHIETA ICT;
- Pirated software;
- Unapproved software; and
- User installed software that does not comply with CHIETA policy.

CHIETA ICT will implement controls to ensure that users are monitored for compliance with the above policy.

25. Network Diagram

A network diagram will be drawn up and maintained to reflect the following:

- Location of computers
- Location of data points
- Location of servers
- Location of external communication equipment
- Network layout
- Switch configuration

- IP addresses and subnet masks

The network diagram will be kept safe and secure by the IT Manager and reviewed Whenever a change to the network is made. An annual review of the network will be undertaken at the end of each financial year to ensure that all changes to the LAN / WAN have been captured on the diagram undertaken at the end of November to ensure that all changes to the LAN / WAN have been captured on the diagram.

26. *Violations and Penalties*

- Should a routine control reveal any infringement of this policy, IT shall issue a warning mentioning the type of infringement detected.
- If subsequent monitoring reveals another infringement, then IT shall give the name of the User and the appropriate details of the infringement to the User's supervisor and Human Resources.
- Systematic infringement of this IT policy will trigger disciplinary sanctions, which can include dismissal.

- The system allows identification of the account and location from where an infringement was carried out, but action shall be taken against a User only if it is clear that they committed the offence; his / her identity is certain; or if they failed to follow the correct security procedures (e.g.: they left their computer open and unattended).
- Should an infringement of the policy lead to technical problems or put the company at risk, the relevant User shall be immediately identified, without prior warning, with the sub standing evidence.
- Should criminal infringements be discovered during monitoring, the records (activity and access logs etc.) shall be secured, and the company may decide to refer the infringement to the relevant authorities.

27. *ICT Help Desk (Problem and Incident Management)*

- All ICT related faults will be logged using an email system.
- When a fault is logged the following will not be omitted
  - Users name
  - Nature of fault
  - Equipment type, software used, system version
- All faults will be categorized into the following levels and solutions will be provided according to these levels:
  - Level 1: Telephonic help by technical assistant
  - Level 2: Only if level 1 is unsuccessful - the technical assistant provides an on-site solution for the user;
  - Level 3: Only if level 2 is unsuccessful - Outsourcing is required to provide a solution for the user;
- It is the responsibility of the IT department to ensure that a technician is always available on the premises . This listing will be updated whenever staff turnover occurs.
- The Technical Assistant will receive a detailed copy of the email containing all the information that is required to repair the fault.

- The IT department technician will complete a report on email of the fault received and the outcome of the report upon completion of the task.
- Calls will only be closed or escalated when the Technical Assistant forwards the email to the IT department with a full description of how the problem was resolved/not resolved.
- On a rotation basis, a Help Desk Assistant will be responsible to attend to this e-mail to close the necessary calls.
- On a daily basis a Help Desk Assistant will do follow-ups. He will phone the user to ensure that the call was attended to and if the user is satisfied. If the user is not satisfied, the call will be re-opened and the technician is notified.
- Monthly service reports will be printed and presented to management. Management will then ensure that all ICT related faults are attended to in a timely manner, and that the resolutions are achieved as per agreement with the service provider. Any issues or outstanding faults will be discussed with the service provider on a monthly basis.

28. ***ICT End User Awareness and Obligations***

- The ICT Department of CHIETA (or the service provider responsible for ICT at CHIETA) will ensure that the contents, application, requirements and obligations of the relevant parties are communicated to the users on a regular basis.
  - The users should be made aware of the following:
  - All ICT related procedures to be followed;
  - Good ICT security practices;
  - Changes to the ICT policy and associated procedures;
  - Non-compliance with the ICT policy and its consequences; and
  - Obligations of ICT end users.
- The users will have the following obligations with regards to ICT at CHIETA:
  - To ensure that they fully understand and comply with the ICT Policy and its repercussions;
  - To use the ICT infrastructure, systems and data in a manner that does not place CHIETA ICT at risk; and
  - To communicate any and all ICT related problems, incidents and security breaches to the ICT Department of CHIETA.

29. ***ICT Policy Maintenance***

- The maintenance of the ICT Policy is the responsibility of the Information and Communication Technology Department of CHIETA.
- The policy should be reviewed continually to ensure compliance with the latest standards and practices to ensure CHIETA’s continual alignment to industry related standards and practices.
- The policy should be formally reviewed, updated, approved and communicated to all relevant CHIETA stakeholders.

30. Responsibilities

It remains the responsibility of end users, line managers and organization structures to collectively ensure that all IT operations comply with this policy. However the CHIETA will carry out regular reviews of information systems and adherence to this policy including assessment by the CHIETA’s Internal Auditors.

Line management is responsible for ensuring that new users are made aware of this policy at the time that they are granted access to the organisation’s systems. The policy will also form an intergraded part of the CHIETA introduction program.

The system manager is responsible for carrying out all related ICT functions as stated in the job profile and makes sure that all ICT protocols and maintenance is functional and in line with the CHIETA policy.