CHIETA
CHEMICAL INDUSTRIES EDUCATION & TRAINING AUTHORITY

HEAD OFFICE
2 Clamart Road, RICHMOND, JOHANNESBURG 2092
PO Box 961, AUCKLAND PARK 2006
Tel: 011 628 7000 | Fax: 011 726 7777
Email: info@chieta.org.za | Website: www.chieta.org.za

ORIGINAL CHIETA DOCUMENT

INFORMATION TECHNOLOGY SECURITY POLICY

TABLE OF CONTENTS

PAGE

1. GLOSSARY OF TERMS

1.1 **Abuse:** The deliberate misuse of privileges which results in a threat to the confidentiality, availability, or integrity of information.

1.2 **Account:** A unique electronic identifier composed of, at minimum, a username and password.

1.3 **Administrator (server):** The individual responsible for installing, maintaining, hardening, logging and reporting on the services running on a server.

1.4 **Archive:** Data that has been removed from the storage system, to another (off-line) location for historical purposes, available for reference or recovery on an as-needed basis. The archive medium may be different from that of the previously stored data, may be in a different physical location, and may, depending on the media and software used, be usable only after it has been run through a "restore" process.

1.5 **Authentication:** The act of identifying or verifying the eligibility of a user or process to access specific categories of information.

1.6 **Authorization:** Following authentication, the granting of access to a resource.

1.7 **Availability:** The property of being accessible and usable upon demand by an authorized user or system.

1.8 **Backup:** A copy of data as it existed at a specific point in time. The backup is held on physically different media (but may be of the same type) as the active data set. Backup data may, depending on the medium and backup software used, be usable only after it has been run through a "restore" process.

1.9 **Breach of Security:** A breach of security occurs when there is a reasonable belief that an unauthorized person has acquired unencrypted electronic personal identity information or other restricted data.

1.10 **Client (systems):** A workstation on a network, typically configured in a Client-Server relationship.

1.11 **Compromise:** Unauthorized disclosure or loss of sensitive information, unauthorized information or system integrity change, or system availability interruption.

1.12 **Confidential Information:** The term confidential information applies broadly to information for which access or disclosure may be assigned some degree of sensitivity, and therefore, for which some degree of protection or access restriction may be warranted. Unauthorized access to or disclosure of information in this category could result in a serious adverse effect, cause financial loss, cause damage to the company's reputation and loss of confidence or public standing, constitute an unwarranted invasion of privacy, or adversely affect a partner, e.g., a business or agency working with the organisation.

1.13 **Confidentiality:** The quality or state of information that prevents disclosure or exposure to unauthorized individuals or systems.

1.14 **Connectivity:** The uninterrupted availability of electronic information paths.

1.15 **Device:** Any electronic component, such as a computer, printer, router, switch, modem, etc.

1.16 **Disaster recovery:** Restoring a system or operational function after a service-impacting event.

1.17 **Electronic Communications:** Electronic communications are any information that is transmitted electronically. This includes, but is not limited to, email and email attachments, web pages, phone calls, faxes, broadcasts, electronically transmitted files, information submitted online, etc. It also applies to details about an individual's online activities, and information from transactional logs.

1.18 **Electronic Information Resource:** A resource used in support of the organisations activities that involves the electronic storage, processing or transmitting of data, as well as the data itself. Electronic Information Resources include application systems, operating systems, tools, communications systems, data – in raw, summary, and interpreted form – and associated computer server, desktop (workstation), portable devices (laptops, PDAs) or media (CD ROM, memory sticks, flash drives), communications and other hardware used to conduct activities in support of the company's mission. These resources are valued information assets of the company.

1.19 **Email Relay:** A service that allows third parties to process an email message where neither the sender nor the recipient is a local user.

1.20 **Email Spam Robot (spam bot)**: A malicious program designed to covertly send unsolicited email (spam) from computers that it infects. The spam bot is remotely controlled as part of a collection, or "army," of spam engines.

1.21 **Email:** Short for electronic mail, the transmission of messages over electronic communications networks.

1.22 **Encryption:** The process of converting data into a cipher or code in order to prevent unauthorized access. The technique obfuscates data in such a manner that a specific algorithm and key are required to interpret the cipher.

1.23 **Enterprise Network:** All devices, cabling, and software which constitute the backbone network, all Local Area and Wireless Networks, and telephone networks.

1.24 **File recovery:** Restoring individual files or records from original, archive or backup media.

1.25 **Firewall:** A device or software application which forms a barrier between a secure environment and an un-trusted environment.

1.26 **FTP:** "File Transfer Protocol." A non-secure method of transferring files between computers on a network. The currently preferred alternative is SFTP.

1.27 **Harden:** The act of configuring a server or client, through the disabling of unnecessary services and application of safeguards, to reduce the likelihood of a system compromise.

1.28 **Host-Based Firewall:** A host-based firewall is software that runs directly on a networked device and protects that device against attack from the network by controlling incoming and/or outgoing network traffic.

1.29 **HTTP:** "Hypertext Transfer Protocol." The communication protocol (language) that enables web browsing.

1.30 **HTTPS:** "Secure Hypertext Transfer Protocol." Acronym used to indicate a secure, encrypted HTTP connection.

1.31 **IMAP:** "Internet Message Access Protocol." A mail protocol that provides access to email and management of email messages on a remote server.

1.32 **IMAPS:** Secure, encrypted IMAP.

1.33 **Incident:** An event that has the potential to compromise the security of a computer system or business process

1.34 **Infected Computer:** A computer containing any type of malicious software.

1.35 **Information Security:** The safeguarding of information against unauthorized disclosure

1.36 **Information Technology:** The hardware and software operated by an organization that processes information on behalf of its stakeholders in order to accomplish a function of the organization.

1.37 **Information:** Data (electronic, paper, etc) which holds value to the organization.

1.38 **Integrity:** The accuracy, completeness, and validity of information in accordance with organizational values and expectations.

1.39 **Interference:** The degradation of a communication signal. Such interference can either slow down a transmission or completely eliminate it.

1.40 **Logging:** The recording of data & events for the purpose of auditing access to systems & services.

1.41 **Malicious Software:** A generic term for software that performs unauthorized activities on a computer, causes damage or allows unauthorized access to be gained. Examples of malicious software include viruses, spyware, and email spam robots.

1.42 **Malware:** Software designed to compromise the confidentiality, availability, or integrity of the system in which it is executed. Viruses and worms are both examples of malware.

1.43 **Misuse:** The accidental or deliberate (abuse) use of privileges which results in a threat to the confidentiality, availability, or integrity of information.

1.44 **Mitigation:** The introduction of safeguards to counter a potential or actual incident.

1.45 **Network Access:** Connectivity which includes the backbone network, all local area and wireless networks, as well as telephone networks.

1.46 **Network Service:** A resource running on a device that can be shared by other computers. Examples include web servers, mail servers, file sharing, remote connectivity capability, DHCP servers.

1.47 **Network:** An integrated, communicating aggregation of computers and peripherals linked through communication facilities.

1.48 **New Server:** A server which has recently been installed and hardened, but has not entered into production status due to pending system scans or firewall rule requests.

1.49 **Password:** A word or string of characters that authenticates a user, a resource, or an access type.

1.50 **Physical Security:** An aspect of information security that addresses the design, implementation, and maintenance of countermeasures that protect the physical resources of an organization. Examples include various locks, fire suppression devices, video cameras, etc.

1.51 **POP:** “Post Office Protocol.” A protocol used to retrieve email from a mail server.

1.52 **Privacy:** The condition of inaccessibility as it relates to personally identifiable information.

1.53 **Process (data):** State of data in which it is being manipulated/changed by an individual, system, or application.

1.54 **Proxy Server:** A server interposed between a client application, such as a Web browser, and a source server.

1.55 **Remote Access:** The ability to remotely connect into a computer via a service running on the device, versus physically at the console.

1.56 **Safeguard:** Protective measures prescribed to meet the security requirements of an information system. Safeguards may include technology features, management constraints, awareness training, physical security, personnel security, among other mitigating factors. Synonymous with security controls and countermeasures.

1.57 **Security Breach:** See "compromise".

1.58 **Sensitive Data:** "Sensitive data" is an informal term used to describe information with some level of sensitivity.

1.59 **Server:** A physical or virtual device which carries out some task (i.e. provides a service) on behalf of yet another piece of software called a client. This includes (but is not limited to) network-aware devices (SNMP, SMB, etc), web servers, proxy servers, file servers, print servers, email servers, etc.

1.60 **Service:** A specific functionality offered/hosted by a server.

1.61 **Session Timeout:** A process that automatically prevents user access to a system or application after a period of inactivity. The purpose of timeouts is to lock out unauthorized users when a system is unattended or when someone forgets to log out of an application.

1.62 **SMTP:** “Simple Mail Transfer Protocol.” The de facto standard for email transmissions across the Internet. SMTP is a text-based protocol, where one or more recipients of a message are specified and then the message text is transferred.

1.63 **SNMP:** “Simple Network Management Protocol.” A protocol used by network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

1.64 **Social Media:** Social media are media for social interaction, using highly accessible and scalable communication techniques. Social media is the use of web-based and mobile technologies to turn communication into interactive dialogue.

1.65 **Spam Bot:** See Email Spam Robot

1.66 **Spyware:** Computer programs that typically track your use and report this information to a remote location. The more malicious spyware programs may capture and report keystrokes, revealing passwords and personal information. Users are often tricked into installing spyware programs without their knowledge. Spyware is sometimes referred to as adware.

1.67 **SSL Certificate:** SSL certificates (certs) are used to confirm the identity of a website or server, encrypt data during transmission, and ensure the integrity of transmitted data.

1.68 **SSL:** “Secure Sockets Layer.” A cryptographic (encrypted) protocol that provides secure communications on the Internet for such things as web browsing, email, Internet faxing, instant messaging and other data transfers.

1.69 **Store (data):** State of data in which it is not in use, but rather it is in storage on media such as (but not limited to) hard drives, backup tapes, USB Drives, or optical media.

1.70 **System:** In general, any interrelated group of electronic components, e.g. hardware and/or software, that works as a coherent entity. With respect to information security breaches, a system is any computer readable collection of information that contains electronic data in an organized form such that information about a particular subject can be distinguished from information about other subjects.

1.71 **Tablet Computer:** Mobile computer that can execute programs, has internet syncing/browsing capability, and is integrated into a flat touch screen interface display. These devices include (but are not limited to) palmtops, Apple iPads, and Android tablets such as the Motorola Xoom and Dell Streak.

1.72 **Telnet:** A network protocol used for connecting to a remote host or server. Telnet is an insecure Internet protocol. The currently preferred alternative is SSH.

1.73 **Transactional Information:** Information, including electronically gathered information, needed either to complete or to identify an electronic communication. Examples include but are not limited to: electronic mail headers, summaries, addresses and addressees; records of telephone calls; and IP address logs. Transactional information does not include the actual contents of people's computers, files, emails, telephone conversations, etc.

1.74 **Transmit (data):** State of data while it is in route between a server and a client.

1.75 **Truncate:** To make shorter. This can be for the purpose of reducing or eliminating the sensitivity of data, such using the last four digits of a Social Security number instead of the entire number.

1.76 **Updates:** Updates “fix" an inherent flaw or security risk in an operating system (the basic program that runs a computer, such as Windows 2000, Windows XP, or Windows 7) or application software. Updates are released on an as-needed basis – typically from the operating system or software vendor (such as Microsoft, Adobe, or Mozilla).

1.77 **User:** Individuals who have been granted access to specific information assets. Users include, but are not limited to, staff, trainees, vendors, volunteers, contractors, or other affiliates of the company.

1.78 **Username:** A unique alpha-numeric identifier associated with a specific user.

1.79 **Virtual Private Network:** A private network which uses encryption and authentication to create a secure channel over un-trusted networks.

1.80 **Virus:** Computer viruses are small, self-replicating computer programs that interfere with computer operation. The effect of viruses can range from negligible to devastating, depending on what the virus program does when it runs. A virus might, for example, corrupt or delete data on a computer, spread itself to other computers, or even install a malicious program.

1.81 **Vulnerability:** A weakness in a system which can be exploited to violate the system's intended behaviour relative to safety, security, reliability, availability, integrity, etc.

2. BACKGROUND

Introduction &General Principles

This policy covers the use of information systems and technologies. This policy also covers the approved software stated in the ICT Policy. 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 has a responsibility to use the CHIETA information technology resources in a manner that service delivery to stakeholders, increases productivity, enhances the CHIETA public image, and is respectful of other employees

2.1 Purpose

2.1.1 The purpose of the Information Technology Policies and Procedures is to:

2.1.1.1 Establish and maintain management and employees accountability for the protection of information Technology resources

2.1.1.2 Promulgate the policy regarding the security of data and information technology resources

2.1.1.3 Define the minimum security standards for the protection of information resources.

2.1.1.4 Define the procedures for usage of Information Technology and Information technology systems in CHIETA

2.1.1.5 This policy shall be adhered to by all CHIETA staff

2.1.1.6 Failure to comply to the IT Policy will be dealt with in line with guidelines specified in the HR Policy

2.2 Compliance

Failure to comply with this policy may result in withdrawal of services, disciplinary action or termination of employment. In such situations, the CHIETA reserves the right to use evidence obtained from computers, voice mail systems or system backups for use in disciplinary proceedings. Such evidence will be deemed to have originated from the user who is responsible for ensuring that access to the service is password protected at all times.

2.3 Management and User Responsibility

2.3.1 Responsibility of Employees

2.3.1.1 Although precautions are taken to safeguard all the systems and data in the CHIETA, functional requirements make it impossible to prohibit all access to it. The employees must therefore take the necessary precautions to ensure that the integrity, confidentiality and availability of all data, systems and equipment are not compromised or abused

2.3.2 Standards – To achieve this the following standards shall apply:

2.3.2.1 Each manager shall ensure that all his or her employees take note of the policy regarding the implementation and maintenance of data and system security.

2.3.2.2 Each manager is responsible for assuring an adequate level of security for all the data and resources that form part of his or her component or team.

2.3.2.3 Each manager shall ensure that the procedures for usage of Information and Information systems in CHIETA will be implemented

2.4 Administrator Accounts

2.4.1 Every division should have an appointed administrator who's roles and responsibilities have been defined in their appropriate procedure. Although we stating that only one administrator per division, CHIETA being a small organization has chosen their working method that enhances service delivery to stakeholders can deviate from this rule and appoint more than one administrator in a division given their business reasons.

2.4.2 In terms of delineation of roles and responsibilities administrators do not normally handle operational duties unless if the risk is declared and reported to the ICT Steering Committee.

Security of ICT Systems

- Generally, employees are given access to the CHIETA's various technologies based on their job functions.
- Only employees whose job performance will benefit from the use of the CHIETA's information technology resources will be given access to the necessary technology. Additionally, employees must successfully complete CHIETA-approved training before being given access to the CHIETA's information technology resources.
- Authorized users of the CHIETA computing and network resources include those who may not work for the CHIETA, but whose access has been authorized by management. Access, passwords, and e-mail accounts are granted by the management of the CHIETA and therefore access to the systems can be denied by management.

3 PHYSICAL SECURITY

3.1 Building Security

3.1.1 Access control – Access control applies to all CHIETA offices, computer rooms and work areas.

3.1.2 Locked doors when offices not in use – __All employees with separate personal offices shall lock the doors when these offices are not in use after hours. The front door to the offices shall be kept locked outside normal office hours.

3.1.3 Controlled access for visitors – __Visitor or other third party access to CHIETA offices, computer facilities, and other work areas containing sensitive, valuable, or critical information shall be controlled by employees.

3.2 Computer Equipment Security

3.2.1 Asset register – All CHIETA computer and communications equipment shall

3.2.1.1 have a unique identifier permanently attached to the equipment

3.2.1.2 Be recorded in the CHIETA's asset register.

3.2.2 Moving equipment – Office computer equipment (desktop computers, fax machines, LAN servers, network hubs, etc.) shall not be moved or relocated without the prior approval of the involved department manager.

3.2.3 **Exception:**

> Equipment which is portable may be moved as long as it is logged in the log out book. (The log out book is owned and managed by CHIETA)

4 LOGICAL SECURITY: POLICIES ON PASSWORD MANAGEMENT

4.1 Password Construction

4.1.1 Minimum password length:

4.1.1.1 A unique string of a minimum of a mix of 8 alpha numeric characters

4.1.1.2 The length of passwords is checked automatically by the system/application when employees construct or select them. The password must contain letters/special characters and numbers.

4.1.2 Must be difficult to guess – Employee-chosen passwords for computers and networks should be difficult to guess. Do ***not*** choose:

4.1.2.1 words in a dictionary

4.1.2.2 proper nouns

4.1.2.3 geographical locations

4.1.2.4 common acronyms

4.1.2.5 slang

4.1.2.6 derivatives of user-IDs

4.1.2.7 common character sequences such as "123456"

4.1.2.8 spouse's name

4.1.2.9 car license plate

4.1.2.10 your ID number/ birth date

without adding unrelated characters.

4.1.3 Guidelines for password construction – Guidelines to help construct employee-chosen passwords.

4.1.3.1 Do ***not*** use control characters and other non-printing characters (which may inadvertently cause network transmission problems or invoke certain system utilities).

4.1.4 The password history size will be set at 6 previous passwords to ensure that the same password is not used consecutively when a change is automatically demanded.

4.1.5 4 Cyclical passwords____Do not construct fixed passwords by combining a set of characters that do not change, with a set of characters that change predictably.

Example:

Characters which change are typically based on the month, a department, a project, or some other easily-guessed factor:

- "X34JAN" in January
- "X34FEB" in February…

4.1.6 Re-use of passwords – __Employees shall not construct passwords which are identical or substantially similar to passwords they have previously used.

4.1.7 Obscuring passwords – The system will obscure the display and printing of passwords so that unauthorised parties will not be able to observe or subsequently recover them.

4.1.8 Forced password changes – All employees shall be automatically forced by the computer system to change their passwords at least once every 45 days. The password change interval will be synchronised across all computer and network platforms at CHIETA

4.1.9 Assignment of initial passwords – The initial passwords issued by the IT Manager are valid only for the involved employee's first on-line session. Once on the system, the employee will be forced to choose another password before any other work can be done.

4.1.10 Limit on entry attempts - After 5 unsuccessful attempts to enter a password within five minutes, the involved employee-ID shall be either:

4.1.10.1 suspended until reset by IT Manager or the IT Technical consultants (in the case of internal connection) or

4.1.10.2 Disconnected (in the case of dial-up or other external network connections).

Action:

> If a user is suspended or disconnected by the system, he/she should contact the IT Manager or the IT Technical consultants.

4.1.11 One user ID – So as to minimise inconvenience for employees, the system is set to ask for only one user-ID and password combination at the time they reach the network and/or destination computer system.

4.1.12 Work-station protection – No bootable passwords shall be used on any CHIETA computers. A bootable password would make the computer inaccessible to other CHIETA staff and so render the machine useless if the employee is away for any reason, and his/her colleagues need to access the computer

4.2 Password-related user responsibilities

4.2.1 Responsibility for user-ID – employees:

4.2.1.1 are responsible for all activity performed with their personal user-IDs

4.2.1.2 shall not allow their employee-IDs to be used by anyone else

4.2.1.3 shall not perform any activity with other employees' IDs.

> **Explanation:**
>
> Sharing employee-IDs and passwords exposes the authorised employee to responsibility for actions that the other party takes with the ID of password.

4.2.2 Different systems – different passwords – To prevent the compromise of multiple systems, employees shall employ different passwords on each of the systems to which they have been granted access, for example the network and the MIS system.

> **Explanation:**
>
> If a hacker were to discover a fixed password, then all the systems to which the individual with the same password had access would be compromised.

4.2.3 Suspected disclosure – If a password is suspected to be known to have been disclosed to unauthorised parties, then the employee shall immediately:

4.2.3.1 act according to the current procedures

4.2.3.2 change all passwords.

4.2.3.3 The IT Manager shall notify the CEO of the password disclosure.

> **Explanation:**

> The basic secure systems design principle behind this policy is that ONLY the user should know his or her password.

4.2.4 Leaving passwords written down – Passwords that have been written down shall not be left in a place where unauthorised persons might discover them.

> **Guidelines:**
> Written passwords can be concealed in a phone number or other seemingly unrelated characters or encoded in some other way.

4.3 User Authentication and Identification

Upon advice from the HR department, the IT Manager will set up the following access protocols:

- Complete new user creation forms
- User name: A unique name composed of an individual's first Initial and Surname
- User Password: A unique string of a minimum of a mix of 8 alpha numeric characters
- Changing user passwords: This will be prompted automatically within 45 days and failure to comply will result in the user account being closed.

Note: The Administrator's account password is a mix of 18 alpha-numeric characters and does not need to be changed on the same frequency.

4.4 Disabling Of User Accounts

HR department will advise the IT Manager of staff resignations / departures through a User Account termination form (HRD-FM-010) so that the user account can be disabled upon departure. **Note:** Locked accounts will be kept "live" for a period of 3 months in order to permit incoming mail to be accessed by authorised officials /successors and to ensure business continuity. Management can advise the IT Manager to keep locked accounts live for a period longer than 3 months via email communication. The transmission / sending capability of these locked accounts will be disabled.

4.5 Inactive User Accounts

As a general rule, all user accounts should be activated at least once in 30 days.
Since inactive accounts are a prime target for intruders, especially if their passwords are compromised, the following will be enforced:

- All user accounts must be reviewed by the IT Manager monthly.
- Accounts that have been inactive for 30 days or more must be disabled by the IT Manager until they are required by the user again.

- Some user accounts may remain open even if inactive until the regional offices are connected to the head office, provided the IT Specialist performs a monthly review to confirm their status.

Special Accounts
All accounts which will be used for service purposes will be defined as per their purpose e.g. recruitment account will have the username recruitment@chieta.org.za
Passwords for these accounts will be set to not expire and will be managed by the appointed individual to access and control that specific account.

5 MANAGEMENT OF COMPUTER VIRUSES

5.1 Introduction

5.1.1 Enterprise anti-virus software must be running and kept up to date on the network. An automatic online update must be scheduled so that the Information Systems gets the latest anti-virus patterns. Enterprise anti-virus is currently installed on the CHIETA Information Systems and an automatic online update is scheduled

5.1.2 Due to the very rapid increase in the number of computer viruses and the ease with which they can be spread, it is essential that CHIETA acts positively to minimise the threat which this poses. The IT department reports on the status of virus checks on a monthly basis through the management report.

5.2 What is a computer virus?

5.2.1 **Definition**

5.2.1.1 A *computer virus* is an unauthorised program which replicates itself and spreads onto various data storage media (floppy disks, magnetic tapes, etc.) and/or across a network.

5.2.2 **Symptoms of infection**

5.2.2.1 The symptoms of virus infection include:

5.2.2.1.1 considerably slower response time

5.2.2.1.2 inexplicable loss of files

5.2.2.1.3 changed modification dates for files

5.2.2.1.4 increased file sizes, and

5.2.2.1.5 total failure of a computer system.

5.2.3 Virus checking at firewalls

5.2.3.1 The IT Department has installed and enabled virus screening software on all CHIETA:

5.2.3.1.1 Firewalls

5.2.3.1.2 FTP servers

5.2.3.1.3 mail servers

5.2.3.1.4 intranet servers, and

5.2.3.1.5 desktop machines.

5.2.3.2 The screening software will immediately detect and eradicate incoming viruses and where possible, CHIETA will notify the senders.

5.2.3.3 Nevertheless, all employees are responsible for having to play their part in containing this threat

5.2.4 Downloading software

5.2.4.1 **Employees shall not down-load software from:**

5.2.4.1.1 dial-up electronic bulletin board systems

5.2.4.1.2 the Internet

5.2.4.1.3 any person or organisation other than a known and trusted supplier

5.2.4.1.4 any other systems outside CHIETA

> **Exception:**
>
> The only exception to this is when software has been downloaded with the assistance of the IT department

5.2.4.2 The IT Department reserves the right to run ad-hoc software checks to ensure that only authorised software is running on CHIETA workstations and laptops.

5.2.5 Employees shall not attempt virus eradication – Employees shall not attempt to eradicate viruses without the expert assistance of the IT Department.

> **Explanation:**
>
> Viruses have become so complex that expert help is essential to:
>
> - avoid employees unwittingly spreading the virus.
> - minimise damage to data files and software
> - ensure that information needed to detect a re-infection has been recorded.

5.2.6 What to do if virus infestation occurs

5.2.6.1 **Procedure:** Follow these steps *immediately* if you suspect infestation by a virus.

5.2.6.1.1 Shut-down the involved computer

5.2.6.1.2 Disconnect from all networks by unplugging the network cable.

5.2.6.1.3 Log with Office Administrator

5.2.6.1.4 Log with IT Technical consultant

5.2.7 Checked stickers:

5.2.7.1 Externally-supplied disks shall not be used on any CHIETA personal computer (PC) or local area network (LAN) server before the Office Administrator:

5.2.7.1.1 checks the disks for viruses

5.2.7.1.2 Applies a sticker that no viruses were found.

5.2.7.1.3 **Note:** Only the Office Administrator may issue this sticker.

5.2.8 Downloaded software:

5.2.8.1 Any authorised software down-loaded from non-CHIETA sources via the Internet shall be screened for viruses (or similar programs such as worms or Trojan horses), i.e. those that you are going to save to disk of files "save as",

5.2.8.2 The IT Department shall ensure that antivirus software is installed on CHIETA workstations and laptops. It runs on an hourly basis.

5.2.8.3 This is the procedure:

5.2.8.3.1 Screen the document *before opening the file,* with an approved virus detection package.

5.2.8.3.2 If a virus is detected, then:

5.2.8.3.2.1 notify the Office Administrator immediately

5.2.8.3.2.2 do not do any further work on the workstation until the virus has been shown to be eradicated.

5.2.9 Prohibition against using excessive resources

5.2.9.1 Employees shall not run or write any computer program or process which is likely to consume significant system resources or otherwise interfere with CHIETA business activities.

5.2.10 No employee involvement with viruses

5.2.10.1 Employees shall not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any CHIETA computer, network, or information. (Such software is known as a virus, bacteria, worm, Trojan horse, and similar names.)

6 COMMUNICATION SECURITY – ELECTRONIC MAIL SYSTEMS

6.1 Business and personal use of mail

6.1.1 Electronic mail systems are primarily for business purposes. Any personal use shall not:

6.1.1.1 interfere with normal business activities

6.1.1.2 involve solicitation

6.1.1.3 be associated with any for-profit outside business activity, and

6.1.1.4 Potentially embarrass CHIETA.

6.2 Privacy issues

6.2.1 Email as private information

6.2.1.1 Employees shall treat electronic mail messages and files as private information.

6.2.1.2 Electronic mail shall be handled as a private and direct communication between a sender and a recipient.

6.2.2 Privacy cannot be guaranteed

6.2.2.1 Internet and other external electronic mail cannot be regarded as private unless encrypted.

6.2.2.2 Users shall not send credit card numbers, passwords, research and development information and other sensitive data via electronic mail unless the material is encrypted.

6.2.3 Disclaimer

6.2.3.1 Although privacy cannot be guaranteed, all emails sent out from CHIETA should carry the disclaimer below the email signature.

6.3 CHIETA records

6.3.1 All messages sent by electronic mail are CHIETA records.

6.3.2 CHIETA reserves the right to:

6.3.2.1 access and disclose all messages sent over its electronic mail system, for any purpose

6.3.2.2 disclose electronic mail messages to law enforcement officials without prior notice to the employees who may have sent or received such messages

6.3.2.3 review the electronic mail communications of employees they supervise to determine whether they have breached security, violated CHIETA policy, or taken other unauthorised actions.

6.3.3 Electronic Signature's

6.3.3.1 User any type of different signature

6.4 Review of mail

6.4.1 All electronic mail sent through the CHIETA mail server is:

6.4.1.1 Routinely scanned by automatic electronic mail content scanning tools to identify selected keywords, file types, and other information.

6.4.2 This means it is subject to review by people other than the recipient and sender.

6.5 Authorisation to read other employees' mail

6.5.1 When the CHIETA CEO deems it necessary, electronic mail messages flowing through CHIETA systems may be monitored for:

6.5.1.1 internal policy compliance

6.5.1.2 suspected criminal activity, and

6.5.1.3 other systems management reasons.

6.5.2 Without the specific authorisation of the above-mentioned managers, all employees shall refrain from electronic mail monitoring tasks.

6.6 Mail retention for future reference

6.6.1 Employee shall if an electronic mail message:

6.6.1.1 contains information relevant to the completion of a business transaction

6.6.1.2 contains potentially important reference information, or

6.6.1.3 has value as evidence of a CHIETA management decision, be retained for future reference.

6.6.2 Most electronic mail messages will not fall into these categories, and so can be erased after receipt. CHIETA must determine how long messages should be kept on record based on legislation.

6.7 Electronic mail as a database

6.7.1 Employees shall regularly move important information from electronic mail message files to word processing documents, databases, and other files.

6.7.2 This is the procedure:

6.7.2.1 Open the mail message that needs to be saved.

6.7.2.2 Select File – Save Attachments.

6.7.2.3 The system will ask for the directory/folder to save the message in. It is recommended to save the messages on the server folder for backup purposes.

6.7.2.4 Please print all relevant information from mail messages.

Explanation:

Electronic mail systems are not intended for the archival storage of important information. Stored electronic mail messages may be periodically expunged by systems administrators, mistakenly erased by employees, and otherwise lost when system problems occur.

6.8 Periodic destruction

6.8.1 While management enforces periodic backups of computer-resident data, internal correspondence shall be disposed of when no longer needed. To this end, all multi-user electronic mail logs shall be destroyed one year after being archived.

6.8.2 Electronic mail messages relevant to current activities, or that are expected to become relevant to current activities, shall be saved as separate files and retained as long as needed by the user.

6.9 Reporting offensive messages__

6.9.1 Employees are encouraged to respond directly to the originator of offensive electronic mail messages, telephone calls, and/or other communications. If the originator does not promptly stop sending offensive messages, employees should report the communications to their manager.

6.10 Junk mail (SPAM)

6.10.1 When employees receive unwanted and unsolicited email (also known as SPAM), they shall refrain from responding directly to the sender. Instead, they should forward the message to the IT Manager IT Technical consultant who will take steps to prevent further transmissions.

6.10.2 CHIETA shall implement antivirus software which automatically creates SPAM folders based on currently recognised SPAM and auto archives affected mails in these folders. However new SPAM are created every day and IT updates the rules manually when new SPAM is reported by CHIETA.

6.11 Broadcasts

6.11.1 Broadcast facilities found in electronic mail systems and voice mail systems -messages that appear on everybody’s computers - may be used only with management approval.

6.12 Scanned signatures

6.12.1 Employees shall not employ scanned versions of hand-rendered signatures to give the impression that an electronic mail message or other electronic communications were signed by the sender.

7 POLICIES FOR USERS

7.1 Other employees’ accounts

7.1.1 Employees shall not use an electronic mail account assigned to another individual to either send or receive messages.

7.1.2 If there is need to read another employee's mail (while they are away on vacation for instance), message forwarding and other facilities shall be used.

7.2 Sender contact information: add a signature

7.2.1 To facilitate communications and to properly identify the sending party, all electronic mail sent using CHIETA information systems shall contain a standard set of sender contact details in a signature line. These will include the sender's:

7.2.1.1 first and last name

7.2.1.2 job title

7.2.1.3 organisational unit, and

7.2.1.4 telephone number.

7.2.1.5 call centre

7.2.1.6 website contacts

7.3 Forwarding and copyright

7.3.1 Unless the information owner/originator agrees in advance, or unless the information is clearly public in nature, employees should adhere to copyright legislation when forwarding electronic mail outside CHIETA's network.

7.4 Obscene, offensive and defamatory remarks

7.4.1 Employees are prohibited from sending or forwarding any messages via CHIETA information systems that:

7.4.1.1 a reasonable person would consider to be defamatory, harassing, obscene or explicitly sexual

7.4.1.2 would be likely to offend on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability.

7.5 Only access to authorised information

7.5.1 An employee may only access and or use the information that he or she is authorised to access/use.

7.6 Shared Directories

7.6.1 The “shared directories” facility shall be used for official purposes only. Private information may not be made available on the network through “shared” directories and/or resources such as CD-ROMs and/or files.

7.6.2 To prevent unauthorised access to information shared through the use of shared directories, users shall always implement password control over the information.

8 INTELLECTUAL PROPERTY

8.1 Intellectual property developed or conceived while an employee is, working is the exclusive property of the CHIETA. This policy includes:

8.1.1 patent

8.1.2 copyright

8.1.3 trademark, and

8.1.4 all other intellectual property rights as manifested in

8.1.4.1 memos

8.1.4.2 plans

8.1.4.3 strategies

8.1.4.4 products

8.1.4.5 computer programs

8.1.4.6 documentation, and

8.1.4.7 other materials.

9 INTERNET CONNECTIONS

The Access to the Internet should be monitored and controlled. The incoming and outgoing e-mails should be filtered for spam's, viruses and profanity etc… IMCF Mail Security software is installed to filter all incoming and outgoing e-mails

CHIETA issues

9.1 Information exchange

9.1.1 CHIETA software, documentation, and all other types of internal information shall not be sold or otherwise transferred to any party for any purposes other than the business purposes expressly authorised by management.

9.1.2 Exchanges of software and/or data between CHIETA and any third party may not proceed unless a written agreement has first been signed by the CHIETA CEO.

9.1.3 Such an agreement shall specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

9.2 **Reading and access to printed confidential information**

9.2.1 Users shall refrain from reading or accessing any unattended, printed document that is marked Confidential and not addressed to the particular user

9.3 Confidentiality

9.3.1 Users shall refrain from reading or accessing any unattended, printed document that is marked Confidential and not addressed to the particular user

9.4 Non-business sites

9.4.1 Employees who discover they have connected with a web site that contains sexually explicit, racist, or other potentially offensive material shall immediately disconnect from that site.

Explanation:

The ability to connect with a specific web site does not in itself imply that employees are permitted to visit that site.

10 USER ISSUES

10.1 If an employee posts a message to an Internet discussion group, an electronic bulletin board, or another public information system, this message shall be accompanied by words clearly indicating that the comments do not necessarily represent the position of CHIETA.

10.2 Such statements are required even when CHIETA's name does not appear in the text of the message and/or when an affiliation with CHIETA has not been explicitly stated.

Exception:

When the CHIETA CEO has approved the message for release.

10.3 Chat rooms and discussion groups

10.3.1 All employees are forbidden from using CHIETA information systems to participate in Internet discussion groups, chat rooms, or other public electronic forums unless expressly authorised by the CHIETA CEO

10.4 Affiliation

10.4.1 When engaged in authorised discussion groups, chat rooms, and other Internet offerings, only those individuals authorised by management to provide official support for CHIETA products and services may indicate their affiliation with CHIETA.

10.4.2 This may be accomplished:

10.4.2.1 explicitly by adding certain words to their messages

10.4.2.2 implicitly via the use of an electronic mail address.

10.4.3 In either case, unless they have received instructions to the contrary, whenever employees disclose an affiliation with CHIETA, they shall clearly indicate that "the opinions expressed are my own, and not necessarily those of my employer."

10.5 Intellectual property rights

10.5.1 Although the Internet is an informal communications environment, the laws for copyrights, patents, trademarks and the like still apply. To this end, employees using CHIETA systems shall:

10.5.1.1 repost material only after obtaining permission from the source

10.5.1.2 quote material from other sources only if these other sources are identified, and

10.5.1.3 reveal internal CHIETA information on the Internet only if the information has been officially approved for public release.

10.6 Political statements/product endorsements

10.6.1 Whenever an Internet user request an affiliation with CHIETA – whether implicitly or explicitly – no political advocacy statements or product/service endorsements shall be made unless the permission of the CHIETA CEO has first been obtained.

10.6.2 It may only be approved by the CHIETA CEO or Liaison manager.

10.7 Identity

10.7.1 When using CHIETA information systems, or when conducting CHIETA business, employees shall not deliberately conceal or misrepresent their identity.

10.7.2 This policy includes participating in authorised discussion groups and chat rooms, as well as establishing accounts on other computers.

11 SECURITY MATTERS

11.1 No direct connection for production computers

11.1.1 In-house production information systems, such as a server, shall not be directly connected to the Internet. Instead these systems shall connect with a commerce server, a database server, or some other intermediate computer that is dedicated to Internet business activity.

11.2 Internet access through firewall

11.2.1 Internet access using computers in CHIETA offices is permissible only when employees go through CHIETA firewall.

11.3 Other ways to access the Internet, such as dial-up connections with an Internet Service Provider (ISP), are prohibited if CHIETA computers are employed.

12 FIREWALL SECURITY

The network must be protected by a firewall (device which protects the network from internal and external hackers). Presently, the CHIETA utilise two firewalls:

- One at the CHIETA head office in Richmond for and
- One at UUNET (for the protection of the two MIS servers)

13 APPLICATION SECURITY

All the critical application software must be protected by user accounts and password against unauthorised users

The following critical applications are protected;

- MIS
- Pastel Accounting
- VIP Payroll and VIP HR
- CHIETA Electronic Fund Transfer (EFT) application Software e.g. Nedbank, Standard Bank etc
- Microsoft Windows Platform

For off shelf software i.e. Pastel and VIP CHIETA accepts their security protocols and logs which come standard with the licensed software.

14 Physical and Environmental Security

Appropriate physical security and access control measures should be established for the IT facilities, including off-site use of information devices in conformance with the general security policy. Physical security and access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), and any other elements required for the system's operation.
Access should be restricted to individuals who have been authorised to gain such access.

The two MIS servers are hosted at a very secure data centre at UUNET in
Woodmead. Currently only persons authorised by the CHIETA have a physical access to these servers.

The server room at the head office will be managed in the following manner;

- Server room is kept in a neat and tidy fashion
- Access to the Server room should be limited to the IT Manager and persons authorized by IT Manager or the CEO.
- A fire prevention system is in place with smoke detectors and gas fire extinguishers.
- The Fire prevention system needs to be annually tested and an approval certificate needs to be recorded by CHIETA.
- A false floor is in place. This helps prevent fire and water damage to the servers.
- No food or drinks will be allowed in the server room.
- All visitors to the server room will be escorted by a CHIETA official, and the visitor will complete a register, clearly stating the date, time and reason for his visit. The entry into the register will be signed off by the CHIETA official, and on a monthly basis, CHIETA management will review the register to verify that only authorised personnel gained access to the server room.
- An approved access list will be developed for access to the server room. This should indicate the people who are currently authorised to access the server room;
- There will be a server room visitor's register to indicate who has gained access to the server room as well as the reason why they are entering the server room;
- The physical security controls to restrict access to the server room will, be increased as and when necessary;
- All servers will be racked in the appropriate manner; and
- The server room should be kept clean and tidy. All chords and cables should be housed in separate trunks.

Updated and approved by the board on 27 March 2014

____

Signature