Ideas to Execution

INDEX

1 INTRODUCTION

1.1 Information Security

Information Security Policies are the cornerstone of information security effectiveness. The Security Policy is intended to define what is expected from an organization with respect to security of Information Systems. The overall objective is to control or guide human behaviour in an attempt to reduce the risk to information assets by accidental or deliberate actions. Information security policies underpin the security and wellbeing of information resources. They are the foundation, the bottom line, of information security within an organization.

We all practice elements of data security. At home, for example, we make sure that deeds and insurance documents are kept safely so that they are available when we need them. All office information deserves to be treated in the same way. In an office, having the right information at the right time can make the difference between success and failure. Data Security will help the user to control and secure information from inadvertent or malicious changes and deletions or unauthorized disclosure. There are three aspects of data security:

Confidentiality: Protecting information from unauthorized disclosure like to the press, or through improper disposal techniques, or those who are not entitled to have the same.

Integrity: Protecting information from unauthorized modification, and ensuring that information, such as a beneficiary list, can be relied upon and is accurate and complete.

Availability: Ensuring information is available when it is required. Data can be held in many different areas, some of these are:

- Network Servers
- Personal Computers and Workstations
- Laptop and Handheld PCs
- Removable Storage Media (Floppy Disks, CD-ROMS, Zip Disks, Flash Drive etc.)
- Data Backup Media (Tapes and Optical Disks)

1.2 Data Loss Prevention

- Leading Causes of Data Loss:
- Natural Disasters
- Viruses
- Human Errors
- Software Malfunction
- Hardware & System Malfunction
- Protection of Hardware from Theft
- Protection of Hardware from Accidental Damage
- Protection of Data from Hardware Loss

Computers are more relied upon now than ever, or more to the point the data that is contained on them. In nearly every instant the system itself can be easily repaired or replaced, but the data once lost may not be retraceable. That's why of regular system backups and the implementation of some preventative measures are always stressed upon.

1.3 Natural Disasters

While the least likely cause of data loss, a natural disaster can have a devastating effect on

the physical drive. In instances of severe housing damage, such as scored platters from fire, water emulsion due to flood, or broken or crushed platters, the drive may become unrecoverable.

The best way to prevent data loss from a natural disaster is an offsite back up. Since it is nearly impossible to predict the arrival of such an event, there should be more than one copy of the system back up kept, one onsite and one off. The type of media back up will depend on system, software, and the required frequency needed to back up. Also be sure to check backups to be certain that they have properly backed up.

1.4 Viruses

Viral infection increases at rate of nearly 200-300 new Trojans, exploits and viruses every month. There are approximately 65135 "wild" or risk posing viruses (source SARC dated Sep 1, 2003). with those numbers growing every day, systems are at an ever-increasing risk to become infected with a virus. There are several ways to protect against a viral threat:

- Install a Firewall on system to prevent hacker's access to user's data.
- Install an anti-virus program on the system and use it regularly for scanning and remove the virus if the system has been infected. Many viruses will lie dormant or perform many minor alterations that can cumulatively disrupt system works. Be sure to check for updates for anti-virus program on a regular basis.
- Back up and be sure to test backups from infection as well. There is no use to restore virus infected back up.
- Beware of any email containing an attachment. If it comes from anonymous sender or don't know from where it has come or what it is, then don't open it, just delete it & block the sender for future mail.

1.5 Human Errors

Even in today's era of highly trained, certified, and computer literate staffing there is always room for the timelessness of accidents. There are few things that might be followed: -

- Be aware. It sounds simple enough to say, but not so easy to perform. When transferring data, be sure it is going to the destination. If asked "Would you like to replace the existing file" make sure, before clicking "yes".
- In case of uncertainty about a task, make sure there is a copy of the data to restore from.
- Take extra care when using any software that may manipulate drives data storage, such as:

  Partition mergers, format changes, or even disk checkers.
- Before upgrading to a new Operating System, take back up of most important files or directories in case there is a problem during the installation. Keep in mind slaved data drive can also be formatted as well.
- Never shut the system down while programs are running. The open files will, more likely, become truncated and non-functional.

1.6 Software Malfunction

Software malfunction is a necessary evil when using a computer. Even the world's top programs cannot anticipate every error that may occur on any given program. There are still few things that can lessen the risks:

- Be sure the software used will ONLY for its intended purpose. Misusing a program may cause it to malfunction.
- Using pirated copies of a program may cause the software to malfunction, resulting in a Corruption of data files.
- Be sure that the proper amount of memory installed while running multiple programs simultaneously. If a program shuts down or hangs up, data might be lost or corrupt.
- Back up is a tedious task, but it is very useful if the software gets corrupted.

1.7 Hardware Malfunction

The most common cause of data loss, hardware malfunction or hard drive failure, is another necessary evil inherent to computing. There is usually no warning that hard drive will fail, but some steps can be taken to minimize the need for data recovery from a hard drive failure:

- Do not stack drives on top of each other-leave space for ventilation. An overheated drive is likely to fail. Be sure to keep the computer away from heat sources and make sure it is well ventilated.
- Use an UPS (Uninterruptible Power Supply) to lessen malfunction caused by power surges.
- NEVER open the casing on a hard drive. Even the smallest grain of dust settling on the platters in the interior of the drive can cause it to fail.
- If system runs the scan disk on every reboot, it shows that system is carrying high risk for future data loss. Back it up while it is still running. ! If system makes any irregular noises such as clicking or ticking coming from the drive. Shutdown the system and call Hardware Engineer for more information.

1.8 Protection of Hardware from Theft

- The Council Server Room is kept locked at all times. Access to the Server Room is restricted and access is only granted when required under supervision of a member of IT Services employees.
- An asset register of computer equipment is maintained by Council employees under whose responsibility the equipment is placed.
- No equipment should be removed from any site without the approval of the IT Manager - except for portable computers that are the responsibility of each named individual user.
- Hardware in particularly vulnerable areas or containing sensitive data should make use of

physical security measures such as locking office doors or installing locking devices to secure hardware to desk.

- Redundant hardware will be disposed of in accordance with the Council Disposal Policy.

1.9 Protection of Hardware from Accidental Damage

- Care should be exercised when eating or drinking near IT equipment. Eating and drinking is not permitted in the Server Room.
- The location of all hardware (computers, printers, modems etc.) should comply with Health and Safety standards including the stability of the desk surface, and elimination of trailing cables. Advice on this can be obtained from the Council's Health and Safety Officer.
- All personal computers and printers should be switched off when not in use for extended periods, such as overnight or during weekends, except for essential Server Room equipment.
- Magnetic media (e.g. diskettes, tapes) should not be placed next to laser printers, photocopiers or telephones as these can cause corruption of the data on the storage media.
- Diskettes/CD ROMS should be labelled and kept in boxes with sensitive diskettes stored in locked desks or fireproof safes.
- Air vents on computers should not be obstructed.

1.10 Protection of Data from Hardware Loss

- Password controls must be implemented. Passwords should have the following Characteristics...
  - Be at least 8 characters long
  - Contain letters and numbers
  - Be different from the previous passwords used
  - Be user generated
- Passwords should be changed...
  - At least once every 40 days
- System password details are recorded by the IT Officers and kept securely.
- Password Protected Screen Savers may be used if required but passwords for screen savers must be notified to IT Services so that access to the PC can be gained if maintenance is required.
- Monitors used in public areas should be tilted away from the public's direct line of sight so that confidential information cannot be viewed.
- Reports containing sensitive information (e.g. Payroll data) which require disposal should be placed in disposal bags for shredding as confidential waste.
- New floppy disks should be used when transferring data to outside organizations.
- Backups and copies of data should be stored securely off-site.
- All storage media, including backups, should be clearly marked to avoid confusion over their contents.
- Where appropriate, physical controls should be used to prevent unauthorized access.

1.11 About Viruses

A virus is a form of malicious code and, as such it is potentially disruptive. It may also be

transferred unknowingly from one computer to another. The term Virus includes all sorts of variations on a theme, including the nastier variants of macro- viruses, Trojans, and Worms, but, for convenience, all such programs are classed simply as virus.

1.12 Viruses tend to fall into 3 groups

Dangerous: - Such as resume and love letter which do real, sometimes irrevocable, damage to a computer's system files, and the programs and data held on the computers storage media, as well as attempting to steal and transmit user ID and password information.

Childish: - Such as Yeke, 'Hitchcock, Flip and Diamond, which do not, generally, corrupt or destroy data, programs, or boot records, but restrict themselves to irritating activities such as displaying childish messages, playing sounds, flipping the screen upside down, or displaying animated graphics.

Ineffective: - Those, such as Bleah, which appear to do nothing at all except reproduce themselves, or attach themselves to files in the system, thereby clogging up the storage media with unnecessary clutter. Some of these viruses are ineffective because of badly written code, - they should do something, but the virus writer didn't get it quite right.

Within all types there are some which operate on the basis of a triggered event usually a date such as April 1st, or October 31st, or a time such 15:10 each day when the Tea Time virus activates.

1.13 Protection of computer from virus infection

- Make regular backups of important data.
- Install antivirus software on computer and use it daily.
- Update the antivirus software with the latest signature files on weekly/fortnightly basis. Antivirus software does no good unless it is frequently updated to protect against the most recent viruses.
- Upgrade the antivirus software when new releases are provided.

Never open or execute a file or e-mail attachment from an unidentified source. If user is unsure of the source, delete it. Recent viruses have been written so that they come from friends and colleagues. Be cautious with attachments even from trusted sources. If it was sent knowingly, an attachment could still contain a virus. Saving it as a file and running the virus scan software will catch any virus that it has been set up to find, therefore will catch most of them.

2 POLICIES FOR GENERAL USERS

2.1 Using Floppies/ CD/ Flash Drives

- Floppy should be used in consultation with system administrator/uncharged computer center and should be scanned before use.
- Unofficial Floppies, CDs or Flash Drives should not be used on office systems.
- Floppy should be write-protected if data is to be transferred from floppy to system.

2.2 Password

- Keep the system screen saver enabled with password protection.
- Don.t share or disclose your password.
- User should not have easily detectable passwords for Network access, screen saver etc.
- A strong password must be as long as possible, include mixed-case letters, include digits and punctuation marks, not be based on any personal information, not be based on any dictionary word, in any language.
- Never use the same password twice.
- Change password at regular intervals.

2.3 Backup

- Backup should be maintained regularly on the space provided on central server of the department or on the storage media as per department policy.
- Keep paper copy of server configuration file.
- Keep the DATs or other removable media in a secure location away from the computer.
- Always backup the data before leaving the workstation.
- For sensitive and important data offsite backup should be used.

2.4 Physical Safety of System

- Protect the system from unauthorized use, loss or damage, e.g. the door should be locked when not in the office.
- Keep portable equipment secure.
- Position monitor and printers so that others cannot see sensitive data.
- Keep floppy disks and other media in a secure place.
- Seek advice on disposal of equipment.
- Report any loss of data or accessories to the System Administrator/uncharged computer center.
- Keep the system and sensitive data secure from outsiders.
- Get authorization before taking equipment off-site.
- Take care when moving equipment (Read instruction on moving equipment).
- Install UPS system with adequate battery backups to avoid any data loss or corruption due to power failure.
- System should be properly shut down before leaving the office.
- Log-off the system if you are leaving your seat.
- Never remove the cables when your PC is powered ON since this can cause an electrical short circuit.
- Do not stop scandisk if system prompts to run it at the time of system start up.
- Always use mouse on mouse pad.
- Be gentle while handling keyboard and mouse.
- Do not open case of the hardware.
- Make sure that there is some slack in the cables attached to your system.

2.5 Computer Files

- All file level security depends upon the file system. Only the most secure file system should be chosen for the server. Then user permission for individual files, folders, drives should be set.
- Any default shares should be removed.
- Only required file and object shares should be enabled on the server.
- Never download or run attached files from unknown email ID.
- Always keep files in the computer in organized manner for easy accessibility. If required create new folders and sub-folders.
- Avoid creating junk files and folders.
- System files and libraries should not be accessed as it can cause malfunctioning of system.
- When transferring data, be sure it is going to the destination. If asked "*Would you like to replace the existing file*" make sure, before clicking "yes".

2.6 General Instructions

- In case of uncertainty about a task, make sure there is a copy of the data to restore from.
- Follow instructions or procedures that come from System administrator/In charge computer center time to time.
- Users are not supposed to do his or her personal work on computers. Please intimate System administrator/Uncharged computer center in case of system malfunction.
- User should always work on his/her allotted machines. In case of any urgency/emergency user may use other's machine with consultation of System administrator/Uncharged computer center.
- Antivirus software should be updated timely in consultation with System Administrator/Uncharged computer center.
- Don.t gives others the opportunity to look over your shoulder if you are working on sensitive data/contents.
- Do not use unnecessary shareware.
- Do not install or copy software on system without permission of System administrator/Uncharged computer center.
- Avoid unnecessary connectivity of Internet.

2.7 IT Security Policy Statements

- The IT Services Section has responsibility for coordinating IT Security. The IT employees must be endowed with sufficient and appropriate authority, allowed direct access to all employees and be capable of establishing the effectiveness of the Council's IT Security procedures.
- Each multi-user computer system 'owned' by the Council will have nominated users who will have day-to-day responsibility for complying with IT Security procedures on that system.
- Personal Computers will be the responsibility of each individual user.
- Employees will be given IT Security awareness training to ensure compliance with this policy and the appropriate legislative requirements.
- Each contract of employment will have a Council Security clause and attached IT

Security
Policy.

- Breaches of IT Security by employees may be considered to be a disciplinary matter.

3 DEPARTMENTAL POLICIES

- Department should have a system administrator or uncharged of computer centre.
- Departmental staff should be aware of I2eConsulting Security policies.
- Department should have its own written security policies, standards and processes, if needed.
- There should be clearly defined system security procedures for the Administrator.
- Personnel in the department should have sufficient authority to accomplish IT security related duties and policies.
- Competent personnel should be available to back up IT security related duties in the event the regular System Administrator is unavailable.
- Department should have a process to address incidents or compromises.
- Computer equipment should be situated safely and free from potential danger (i.e. leaky roofs etc.).
- Uninterruptible Power Supplies (UPS) should protect servers and workstations.
- Heating, cooling and ventilation should keep your systems at the appropriate temperature and humidity.
- Department should have plans to use software that enforces strong passwords.
- There should be written procedures for forgotten passwords
- Physical security audit should be conducted.
- Department should have physical security standards and procedures.
- There should be procedures for locking IT offices, telephone closets and computer rooms.
- Department should have an alarm system.
- Accesses should be secure when offices/departments are vacant.
- Workstations and laptops should be locked down to deter theft.
- Department should have a network map/diagram of the LAN (Local Area Network).
- There should be a partnership with vendors who can help in an emergency if your equipment is damaged due to disaster.
- Backup files should be sent off-site to a physically secure location.
- Department should store media off site.
- Environment of a selected off-site storage area (temperature, humidity, etc.) should be within the manufacturer's recommended range for the backup media.
- Department should have a configuration/asset control plan for all hardware and software products.
- Trained authorized individuals should only be allowed to install computer equipment and software.

3.1 Department Officer Responsibilities

- Ensuring that all IT systems in use are appropriately assessed for security compliance and are protected in accordance with the IT Security Policy.

- Ensuring that the Council IT security standards are implemented effectively and regularly reviewed.

- Monitor compliance with the Data Protection Act (1998), including the maintenance of the Councils Notification, and ensuring the adequacy of arrangements for the physical security of computers and contingency planning.
- Responsible for the receipt of all data requests for Subject Access under Data Protection Act (1998); monitoring the procedures for fulfilling such requests, ensuring that the information supplied for the tracing of the data is sufficient, and ensuring the disclosure of the relevant information to the applicants within the specified time scale. (to be established)
- Responsible for ensuring that the Council's employees, servants or agents are kept aware of the requirements of the Data Protection Act (1998) and their responsibilities under it.

3.2 IT Officers

- Providing a focus within the Council on all IT security matters.
- Receiving and considering reports of IT security incidents, initiating appropriate action and passing the reports to the Council IT Manager.
- Playing a proactive role in establishing and implementing IT security procedures and employees awareness.
- Assisting the IT Manager in monitoring the effectiveness of IT security within the Council and initiating any requested changes to security procedures which become necessary as a result of the monitoring process.
- Ensure that regular backups are taken and stored appropriately off-site.
- Ensure that appropriate levels of access are granted to system users.
- Ensure that all Council employees using the systems are aware of their IT Security responsibilities and receive awareness training on same.
- Monitor IT Security and report IT Security Incidents to the IT Manager and take action where appropriate.

3.3 Users

- Comply with the Council IT Security Policy.
- Comply with Legislation and Guidelines in Section 1.2.
- Notify immediately the IT Manager or the IT Officers of IT security breaches which come to their attention.
- Notify immediately the IT Manager of any Data Protection breaches that come to their attention.

4 SECURITY POLICY FOR PURCHASE

4.1 Hardware

"All purchases of new systems and hardware or new components for existing systems must be made in accordance with Information Security and other Organization policies, as well as technical standards fixed by the govt. Such requests to purchase must be based upon a User Requirements Specification document and take account of longer term organizational operation's needs." The purchase of new computers and peripherals requires careful consideration of

operations needs because it is usually expensive to make subsequent changes. Information Security issues to be considered, when implementing the policy, include the following:

- Approval of purchase of New System Hardware
- The system must have adequate capacity or else it may not be able to process the data.
- Where hardware maintenance is poor or unreliable, it greatly increases the risk to the organization, because, in the event of failure, processing could simply STOP.
- User requirement specification including deployment and use of available resources and Proposed use of new equipment's.

5 SECURITY POLICY FOR ACCESS CONTROL

Policy for access control defines access to computer systems to various categories of users. Access Control standards are the rules, which an organization applies in order to control, access to its information assets. Such standards should always be appropriate to the organization's operation and security needs. The dangers of using inadequate access control standards range from inconvenience to critical loss or data corruption.

Security for Access Control depends upon following points:

5.1 Managing Access Control Standards

"Access Control standards for information systems must be established by management and should incorporate the need to balance restrictions to prevent unauthorized access against the need to provide unhindered access to meet operational needs."

Information Security issues to be considered, when implementing the policy, include the following:

- The lack of uniform standards controlling the access to information and systems, can lead to disparities and weaknesses.
- Where access control is not modified in response to enhanced sensitivity of processed information, the risk of a breach to its confidentiality will increase perhaps substantially.
- Access control standards that are too tight or inflexible can impede the department's day-to-day activities and frustrate staff.

5.2 Managing User Access

"Access to all systems must be authorized by the owner of the system and such access, including the appropriate access rights (or privileges) must be recorded in an Access Control List. Such records are to be regarded as Highly Confidential documents and safeguarded accordingly."

Good management of user access to information systems allows to implement tight security controls and to identify breaches of Access Control standards.

Information Security issues to be considered, when implementing the policy, include the following:

- Lack of a managed access control procedure can result in unauthorized access to information systems thereby compromising confidentiality and potentially the integrity of the data.
- Logon screens or banners, which supply information about the system prior to successful logon, should be removed as they can assist unauthorized users to gain access.
- Where regulation and documentation of Access Control has been informal, this can frustrate the re-allocation of duties because there are no records of current access rights and privileges.
- Allocating inappropriate privileges to inexperienced staff can result in accidental errors and processing problems.

5.3 Securing Unattended Workstations

"Equipment is always to be safeguarded appropriately – especially when left unattended."

Computer equipment, which is logged on and unattended can present a tempting target for unscrupulous staff or third parties on the premises. However, all measures to make it secure should observe the Access Control policy.

Information Security issues to be considered, when implementing the policy, include the following:

- Unauthorized access of an unattended workstation can result in harmful or fraudulent entries, e.g. modification of data, fraudulent e-mail use, etc.
- Access to an unattended workstation could result in damage to the equipment, deletion of data and/or the modification of system/ configuration files.

5.4 Managing Network Access Controls

"Access to the resources on the network must be strictly controlled to prevent unauthorized access, Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized."

Connections to the network (including user's logon) have to be properly managed to ensure that only authorized devices / persons are connected.

Information Security issues to be considered, when implementing the policy, include the following:

- Unauthorized access to programs or applications could lead to fraudulent transactions or false entries.
- Where physical or logical access has not been controlled, users may find (and exploit) unintentional access routes to systems and network resources. For example: they connect a laptop to a wall socket, bypass the login server, and connect directly to the main server.
- Unauthorized external access to the network will usually result in damage, corruption and almost certain loss of confidentiality of information. Such hacks are usually motivated by malicious or fraudulent intent.
- Incomplete or incorrect data in a user's network access profile could result in their being permitted to modify, delete, or have access to, confidential information on inappropriate network resources.
- Modification made to a network access profile without adequate change control procedures

in place could result in unexpected (and probably accidental) access to unauthorized network resources.

- User ID that suggests their privileges (e.g. a user ID of .allprivs.) may invite hackers to try hard to crack their password.
- Connections to a third party network (e.g. in e-commerce situations), cannot only possibly introduce viruses, but can also disrupt business operations where data is inadvertently transmitted into the network.

5.5 Controlling Access to Operating System Software

"Access to operating system commands is to be restricted to those persons who are authorized to perform systems administration / management functions. Even, then such access must be operated under dual control requiring the specific approval of senior management."

The operating system controls a computer's operation; .pre-loaded. With it are commands and utilities which set-up and maintain the computer's environment. All systems, from PCs to large servers, should be hardened to remove all unnecessary development tools and utilities prior to delivery to end-users.

Information Security issues to be considered, when implementing the policy include the following:

- Staff with access to the command line, could succeed in executing system commands, which could damage and corrupt the system and data files.
- Operating system commands could be used to disable or circumvent access control and audit log facilities, etc.

5.6 Managing Passwords

"The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guideline. In particular, passwords shall not be shared with any other person for any reason."

Most computer systems are accessed by a combination of User ID and password. This policy discusses the management of passwords from an administrator's perspective.

Information Security issues to be considered, when implementing the policy include the following:

- Password allocation via the System Administrator or other technical staff can compromise access control during which time unauthorized access may take place. This will be an unacceptable risk for highly sensitive systems.
  - Passwords that are shared may allow unauthorized access to the information systems.
- Users who need to access multiple systems may keep a hand written note of the different passwords- e.g. in a diary- especially where they are changed frequently. However, such insecure records make an easy target for ill-intentioned persons wishing to break into the system.

5.7 Securing Against Unauthorized Physical Access

"Physical access to high security areas is to be controlled with strong identification and authentication techniques. Staff with authorization to enter such areas is to be provided with information on the potential security risks involved."

Personal who work in, or have access to, high security areas may be put under pressure to reveal access codes or keys, or to breach security by performing unauthorized/illegal tasks, such as copying confidential information. The organization should provide adequate information regarding, and safeguards to prevent, such eventualities.

Information Security issues to be considered, when implementing the policy include the following:

- A member of staff may be threatened or coerced to disclose confidential access codes/ Procedures or information about the organization's systems.
- A member of staff may be threatened or coerced outside the work place to disclose confidential access codes/ procedures or information about the organization's systems.

Security aspects should be designed in such a manner that the responsibility of high security data can be accessible among various officers. In case security breach occurs at one level it can be prevented on other levels. The application should have multilevel password authentication, i.e. the data could be accessible only after authentication by group of authorized personnel.

5.8 Restricting Access

"Access controls are to be set at an appropriate level which minimizes information security risks yet also allows the organization's business activities to be carried without undue hindrance."

Access to systems and their data must be restricted to ensure that information is denied to unauthorized users.

However, inappropriate restrictions could result in individual users being unable to do their job, and cause delays and errors in legitimate data processing. Similarly, excessive privilege could allow an authorized user to damage information systems and files, causing delays and errors.

Information Security issues to be considered, when implementing the policy, include the following:

- Excessive systems privileges could allow authorized users to modify (or, more likely, corrupt/destroy) the operating system configuration and application software setting with grave results.
- Lack of access restrictions could: -
  - Allow staff and third parties to modify documents and other data file.
  - Risk loss of confidentiality and integrity, and also possible legal for potential infringements of the Data Protection Act or local equivalent.

5.9 Monitoring System Access and Use

"Access is to be logged and monitored to identify potential misuse of systems or information."

System access must be monitored regularly to prevent attempts at unauthorized access and to confirm that access control standards are effective.

Information Security issues to be considered, when implementing the policy, include the following:

- Without frequent monitoring, it is difficult to assess the effectiveness of access controls. Unauthorized access can remain undetected, enabling knowledge of this .security hole. to be passed to persons with possible malicious or fraudulent intent. The consequences can be serious.
- Without hard evidence of a security breach, it is difficult to take disciplinary action, and it may be impossible to take legal action.

5.10 Giving Access to Files and Documents

"Access to information and documents is to be carefully controlled; ensuring that only authorized personal may have access to sensitive information."

Information Security issues to be considered, when implementing the policy, include the following:

- With poor or inadequate access control over documents and files, information may be copied or modified by unauthorized persons, or become corrupted unintentionally or maliciously.
- Where the Access Control is seen as overly restrictive, users could be tempted to share Privileged accounts (login + password) in order to access information.

5.11 Managing Higher Risks System Access

"Access Controls for highly sensitive information or high risk systems are to be set in Accordance with the value and classification of the information assets being protected."

High risk systems require more stringent access control safeguards due to the confidentiality of the information they process and / or the purpose of the system e.g. the funds transfer systems used by banks. Ideally, the operating systems for such systems should be hardened to further enhance security.

Information Security issues to be considered, when implementing the policy, include the following:

- Access to a critical system from a workstation external to its designated operation area can threaten its integrity and safety.
- Access control. Both physical and logical should be measurably higher than for other systems.
- Dual control and segregation of duties should be considered for all functions.
- Privileges should be reduced to the lowest level to reasonably perform the job concerned.
- Personal should be carefully selected with their records vetted for suitability for such jobs.

5.12 Controlling Remote User Access

"Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques."

Remote users, either tele-workers or personal on official trips etc., may need to

communicate directly with their organizations systems to receive/send data and updates.

Such users are physically remote, and they will often be connecting through public (insecure) Networks. This increases the threat of unauthorized access.

Information Security issues to be considered, when implementing the policy, include the following:

- The use of a User ID and password as the sole means of access control may provide inadequate security to enable access to the organization's system especially where telephone dial up access is permitted.

5.13 Recommendations on Accounts and Passwords

- Passwords should be changed frequently.
- Department should have an account removal process for persons who have gone out of department.
- Department should have a method for identifying unauthorized users. Regular cross checking should be done to make sure the presence of authorize user. This can be done through verifying with other maintained data like attendance record etc.
- Staffs should receive computer security awareness training.
- Department should maintain a Document of identities, having root access to departmental information.
- Department should maintain the identity of those having remote access to departmental information.
- There should be written procedures for closing accounts when an employee terminates Employment or moves out of the department.

5.14 Protection of Remote Access Facility

- The telephone numbers for Remote Access should not be published in telephone directories for general circulation or disclosed to anyone.
- Remote access equipment is situated in the Server Room.

6 SECURITY POLICIES FOR NETWORKS

6.1 Configuring Networks

"The network must be designed and configured to deliver high performance and reliability to meet the needs of the operations whilst providing a high degree of access controls and range of privilege restrictions."

The configuration of network impacts directly on its performance and affects its stability and information security.

Information security issues to be considered, when implementing the policy, include the following:

- Poor network stability can threaten operations.
- Inadequate control over access to network can jeopardize the confidentiality and integrity of data.

- Slow or inadequate system response times impede the processing.

6.2 Managing the Network

"Suitably qualified staffs are to manage the organization's network, and preserve its integrity in collaboration with the nominated individual system owners."

All but the smallest networks, where changes are relatively infrequent, require on-going management.

Information security issues to be considered, when implementing the policy, include the following:

- Inappropriate control over access to the network will threaten the confidentiality and integrity of data.
- Inadequate capacity can make efficient operation difficult or impossible.
- Slow or inadequate system response times impede the processing.

6.3 Accessing Network Remotely

"Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted."

Remote access is traditionally provided by means of dial-up or leased phone lines. However, the Virtual Private Network provides access across public networks, e.g. the Internet.

Information security issues to be considered, when implementing the policy, include the following:

- Inadequate Internet Security safeguards can allow unauthorized access to the network, with potentially disastrous consequences.
- Weak dial-in-security standards can give unauthorized access to the network, the consequences of which could be very serious.

6.4 Defending Network Information from Malicious Attack

"System hardware, operating and application software, the networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion."

The measures should be taken to defend computer hardware against physical damage and software from unauthorized usage.

Information security issues to be considered, when implementing the policy, include the following:

- Hardware can be physically damaged, through a malicious act, perhaps necessitating a system close down or delayed operations.
- Unauthorized and inappropriate use of software can lead to malicious and/or fraudulent amendment of data.

6.5 Recommendations on Network and Configuration Security

- Department should have an inventory of devices attached to the network.

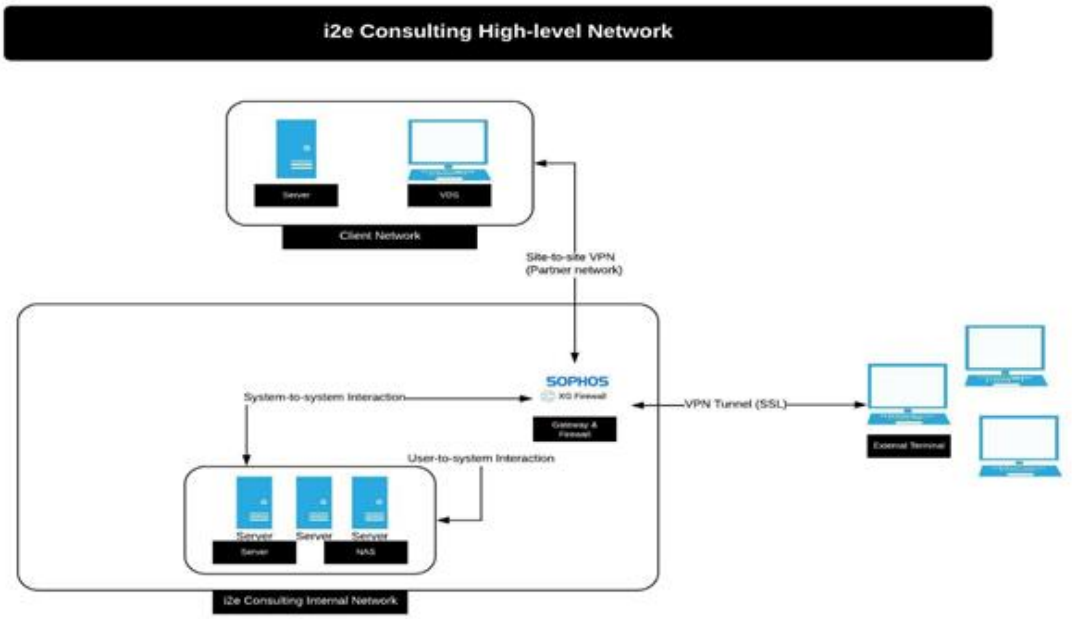
The room jacks should be mapped to a switch port.

- There should be a policy as to how network services are accessed by users.
- Department should have network documentation to assist problem resolution of a computer or network device.
- Department should have the ability to continue to function in the event of a wide area network failure.
- Department should have a network diagram that includes IP addresses, room numbers and responsible parties.
- End users should be prevented from downloading and/or installing software.
- Contents of system logs should be protected from unauthorized access, modification, and/or deletion.
- CD-ROM Auto run feature should be disabled on all workstations.
- Trusted workstations should be secured if used for other purposes.
- Trusted workstations should be SSL or VPN enabled.
- Trusted workstations should be required to have complex passwords.
- Security precautions should be taken for dial-in modems.
- Administrator account, and any equivalent accounts, on all workstations should be limited to the office technical support person.
- File sharing should be properly permitted and secured on any workstation in the department.
- File sharing should be "unbound" from TCP/IP transport (to prevent access from the Internet) while leaving it bound to NetBEUI for local transport.

6.6 Recommendation on Host based firewall

- Someone should monitor if anyone is accessing critical data.
- There should be process for managing individual firewalls on all desktops.
- Settings should be password protected.
- Logs should be often reviewed.
- There should be central monitoring of settings and logs.

6.7 Network Diagram



7 SECURITY POLICY FOR OPERATING SYSTEM

Computer programs that are primarily or entirely concerned with controlling the computer and its associated hardware, rather than with processing work for users are known as Operating System. Computers can operate without application software, but cannot run without an Operating System.

"Operating Systems must be regularly monitored and all required 'housekeeping' routines adhered to."

The operating system of desktop systems within departments will generally run without substantial interference. However, for servers, mini-computers and mainframes, especially those running mature Operating Systems (OS), day to day housekeeping is usually required.

Information security issues to be considered, when implementing the policy include the following:

- Where an upgraded operating system fail to perform as expected, this can result in a loss of stability or even the total failure of some systems.
- Where housekeeping and routine support are informal or incident led, weaknesses in the security safeguards can go undetected and offer the potential for fraud or malicious damage.

8 SECURITY POLICY FOR SOFTWARE

8.1 Managing Operational Program Libraries

"Only designated staff may access operational program libraries. Amendments may only be made using a combination of technical access control and robust procedures operated under dual control." Managing the directories within computer(s) in which operational (live) software is stored. Information security issues to be considered, when implementing the policy, include the following:

- If operational program libraries are poorly protected, software and configuration files could be modified without authorization, resulting in disruption to system and / or other incidents.
- Unauthorized use of production software can cause disruption to systems or fraud against the department.

8.2 Managing Program Source Libraries

"Only designated staff may access program source libraries. Amendments may only be made using a combination of technical access control and robust procedures operated under dual control. Managing the directory areas within the system where the source code, object code of live and development systems are held. Live and development libraries must always be kept separate."

Information security issues to be considered, when implementing the policy, include the following:

- Lack of the source code can make it difficult or impossible to maintain the systems.
- Unauthorized amendment of source code can result in system failures and/or malicious damage.

8.3 Controlling Program Listing

"Program listing must be controlled and kept fully up to date at all time." Controlling includes taking printouts, reports, electronic or hard copy of the application source code that makes up the programs run on the systems.

Information security issues to be considered when, implementing the policy, include the following:

- Loss or unavailability of a listing can result in delays in identifying the source of a system problem, the result of which could be severe.
- Having a program listing available can be used by anyone with ill intent or seeking to defraud, as it gives them the precise logic and routines for the system in question.

8.4 Controlling Program Source Libraries

"Formal change control procedures with comprehensive audit trails are to be used to control program source libraries." Monitoring and investigating changes made to program source libraries.

Information Security issues to be considered, when implementing the policy, include the following:

- Any unauthorized changes made to the program source libraries can open the door to potential error or fraud.
- If audit trail reports and event logs are not regularly reviewed, incidents can remain undetected.

8.5 Controlling Old Versions of Programs

"Formal change control procedures with comprehensive audit trails are to be used to Control versions of old programs." Controlling the way, in which user handle the application code of programs within the system, which has been superseded or discontinued.

Information Security issues to be considered, when implementing the policy, include the following:

- If the program library has been removed or updated, user may not be able to access or

revert to the older version of the application if need be. This could cause severe problems where there are found to be major bugs in the newer version.

- Beware of old versions of programs being confused with the latest version, resulting either in the loss of recent enhancement or a failure of other systems, which depend on recent features.

9 SECURITY POLICY FOR CYBER CRIME

"Security on the network is to be maintained at the highest level. Those responsible for the network and external communications have to receive proper training in risk assessment and how to build secure systems which minimize the threats from cybercrime."

There is a very high risk of external security breaches where network security is inadequate.

Information security issues to be considered, when implementing the policies, include the following:

- Criminals may target departments information system, resulting in serious financial loss and damage to department .s operations and reputation.
- Cybercrime is an ever-increasing area of concern, and suitable training is to be given to those persons responsible for network security to minimize such risks.

9.1 Recommendations On to Web Servers and Email

- Web server should be set to only accept traffic on port 80.
- Web server should be set to reject attempts to remotely administer it.
- Web server should be set to authenticate certain user traffic.
- FTP servers should be set to authenticate users
- Traffic should be encrypted/secured
- E-mail server should be set to scan mail and attachments for viruses.
- E-mail server should be set to reject attachments.
- E-mail server should be set NOT to act as a relay.
- Web access to e-mail should be secured.
- Client connections from outside the subnet should be secured/encrypted.

9.2 Using the Internet

Use of the Internet by employees that can be deemed to be of an illegal, offensive or unethical nature is unacceptable and therefore just cause for taking disciplinary action e.g.

- Violation of copyright, license agreements or other contracts for example copying and using software for business purposes from a site where there is a clear limitation for personal use only;
- Downloading or viewing any information which could be considered illegal or offensive e.g. pornographic or racist material;
- Successful or unsuccessful attempts to gain unauthorized access to information resources -

  Commonly known as
  'hacking';

- Using or knowingly allowing someone else to use any computer, computer network, computer system, program or software to devise or execute any artifice or scheme to defraud or to obtain money, property, services, or other things of value by false pretences, promises or representations;

No file should be downloaded from or via the Internet unless doing so is expressly permitted by the IT Manager and it is in connection with the user's job. Particular attention must be paid to any specified licensing specifications or other similar conditions. Employees are not permitted to enter into any agreement on behalf of the Council.

10 USE OF E-MAIL

10.1 Introduction

Increasingly e-mail is being seen as the preferred mechanism for communicating not only internally within an organisation but also externally to other organisations outside the Council. While it would be foolish to ignore the obvious advantages to all parties in using this technology, particularly in view of the fact that others external to this organisation initiate many contacts using this method, employees must accept the need to be professional in approach whenever communicating externally, irrespective of the medium.

Unlike other forms of communication there are also special security issues with e-mail including the inadvertent introduction of computer viruses and the danger of messages being read by other than the intended recipient. This is particularly so for e-mail that may be sent or received via less secure networks such as the Internet.

All employees must follow the policy as per company standard IT policy applies to any electronic mail whether internal or issued to or received from external sources and it applies equally to Internet mail as well as normal e-mail facilities.

The actual policy statements are contained in Appendix D to this document however the paragraphs below explain the reasoning behind the policy to enable employees to have a clear understanding of the need for such rules and guidelines.

10.2 Outgoing Email - Tone and Content

Writing a letter and having it typed on headed notepaper almost automatically instils a 'formality of tone' on the author, and this is a good thing (but not forgetting the spirit of the 'Plain English' campaign). However, e-mail almost has the exact opposite effect. Tone and content tend to be much more relaxed and humor can be the norm and this is not necessarily a good thing when dealing with outsiders. Email is not a written telephone conversation. It is difficult to put a laugh into your words even if you were smiling when you wrote them!

Care too needs to be taken when responding to an e-mail. The tone of response is often dictated by the tone of the originating message, nevertheless, without being bureaucratic or stilted or needlessly formal, frivolous e-mail should be avoided even where the original message may itself appear to be frivolous.

Email being sent externally, and even e-mail being sent to another department within this organization, that is dealing with business matters, i.e. not messages confirming the date and time of a meeting for example, should not be treated any less formally than more traditional paper-based methods of communication and, if appropriate, should be approved before dispatch in the same way as a draft letter may require approval. Clear and succinct language should be used and the same

standard of grammar and spelling should be applied in the same way that they would be applied to letters on headed stationery. Obviously it is not necessary to begin with 'Dear ...' or finish with 'yours sincerely ....'

10.3 Outgoing E-Mail - Security

The route by which e-mail is delivered is often circuitous and may even involve being exposed to very insecure networks. Users should remember that e-mail messages can be intercepted due to the nature of the internet. It is possible to set up routines that can scan passing e-mail for key words without being detected - the Internet equivalent of phone tapping. Consequently, employees should give very serious consideration to the contents of any message or attachments sent by e-mail.

10.4 Incoming E-Mail

Know whom you are talking to. Although this may seem to be an obvious thing to do employees should always read who sent the message before reading, and perhaps reacting to, the message itself.

11 BACKUP POLICIES

System administrator or the nodal officer will be responsible for developing a regimen for backing up the systems depending upon configuration, software applications, nature of data and other factors. These regimens must be documented and made available to users for references. Administrator will also ensure these procedures are followed strictly and implemented as per rules.

Departments will ensure their Backup media / devices such as tape Drives, CD-ROM, and Flash Drives etc. for necessary backup. Departments should also try to set infrastructure for taking backup over the network for their Sub-Offices. Remote Backup Services could also be taken for backup and recovery important data using a secure and trusted server on the Intranet.

Departments should maintain backup infrastructure, including upgrading the hardware and software as needed.

11.1 Backup Process

"The purpose of backup is to protect the files on the disks from catastrophic loss. The backup of disk files is performed on a daily basis to protect data from being lost due to a hardware or software malfunction. "
The individual user is responsible for ensuring the necessary and regular backup of document files of his/her own computer.

Here are some policies and guidelines to keep in mind:

For Individual Desktop

- The user should keep original application diskettes or CDs for specialized software, along with licensing information, in case any of that software needs to be reinstalled.
- Backup should be taken on removable storage media or devices such as Zip drives, floppy

  Disks, CD-ROM, Flash Drives etc. (refer annexure for details of these devices)

Appropriate backup software can also be used for taking regular backups.

- Users and/or their departments are responsible for purchasing removable media (e.g. Zip disks, etc.)
- In case of lost or damaged system files and standard applications, user is required to call System administrator/IT Nodal Officer for solution.

To ensure the safety of their backup files, users should:

- Keep very important backup under lock and key. However one copy may be kept in another building if possible, for restoration purpose.
- Keep documents in an appropriate folder and assign similar names for easy backup.
- Back up entire Documents/ folder to the removable media at least once a week or daily if documents are frequently created/changed.
- Maintain at least 2 backup sets, alternating their use. Thus if latest backup goes bad, there will still be the other backup of older version.
- Tapes can be reused, but with time as quality of a tape degrades, proper precautions must be taken. If a tape goes bad, mark it as bad and discard it.

For Network Users

Users connected to LAN will be allocated storage area on a network server. This storage area will be usually a separate drive and, maintained by system administrator or a person nominated as a nodal officer for that department. This drive will contain folders or directories by the same name of system, which can then be accessed in explorer by giving correct password. Files can be copied from the user's workstation to this folder. These drive folders should be backed up to magnetic tape (DAT), and the tapes should then further backup to an off-site storage facility provided for security and disaster recovery. It is strongly recommended that the backup tapes should be kept in a far off building.

File Backup

The Share drive folders should be backed up to magnetic tape cartridges each weekday night.

Off-site Storage

In order to provide disaster recovery capability, backup tapes should be backed up to a secure off- site storage facility.

The backup tapes should be maintained in off-site storage according to the following schedule:

- Weekday tapes should be stored off-site for two weeks.
- Monthly tapes should be retained off-site for one year.
- Fiscal Year End and Calendar Year End tapes remain off-site for five years.

11.2 Restoration Process

The primary file restore process is to recreate the disk area as of the last backup operation.

The restoration process in most cases simply replays the backup recordings, starting with a base level backup and adding incremental backups as necessary, to rebuild the information.

If the required backup tape is on-site, files can usually be restored within a few hours or less. If the tape has been called from off-site storage, it can be called in days' time. User is required to furnish following information, which is necessary to expedite the restoration process.

- User's name and telephone number.
- The name of the workstation or personal computer including the administrative "domains" and other related aliases.
- The name of the disk area, partition and volume involved.
- The source of file losses (accidental removal, disk failure).
- The current status of the affected disk area, partition or volume.
- Indicate the date of the last known good version of the file. This would help to identify the set of backup tapes to use in attempting to restore the file.
- If e-mail needs to be restored, indicate the name of the user's mail server, the User name used to log on to the mail server, and the date, subject, etc. of the email.

In the case of minor file loss, like accidental removal, additional information is needed:

- The complete filenames of the lost files.
- The time, files were last modified (or created).
- The time, files were lost or destroyed

If the user needs an archived tape, kept off-site, it is very important that the user should have the following information because of the significant cost involved in retrieving and restoring them:

- The name of the computer at the time of the backup.
- The month(s) and year of the backup

11.3 Recommendations on Backup and Recovery & Disaster Planning

- Files should be kept on-site in a secure location.
- Critical files should be regularly backed up.
- Backup files should be periodically restored as a test to verify they are usable.
- There must be a written contingency plan to perform critical processing in the event that on-site workstations are unavailable.
- There should be a plan to continue departmental working in the event when the central systems are down for an extended period.
- Contingency plan should be periodically tested to verify that it could be followed to resume critical processing.
- Critical data should be stored on a department server to protect from compromise.

12 LAN SECURITY

As indicated earlier the office has to have a separate policy for stand-alone PCs in addition to the LAN security policy. In the event of a conflict, the network policy supersedes the stand-alone

policy. All employees of the department are required to read this policy and follow the procedures therein.

This network policy addresses the following specific issues:

- Documentation of Network Applications and System Software.
- Data confidentiality, integrity, and availability over the network.
- Frequency and retention periods for network backup
- Authorized use of network resources
- Adherence to software licensing agreements
- Network Hardware maintenance
- Problem logging/reporting and monitoring
- User responsibilities for security, workstation maintenance, and backup of data files
- Prevention and detection of network viruses

12.1 Network Organization

This section covers key definitions that are used in this policy and describes the departmental structure relating to PCs and LANs.

(A) Definitions

Personal Computer (PC) (also called Node): A small computer containing a motherboard with a Central Processing Unit (CPU), memory chips, associated supporting processors, and slots, sockets, or plugs for attaching peripheral equipment, such as a keyboard, video monitor, floppy disk, and hard disk. PCs may be used as stand-alone workstations as a client in a network, or as a terminal for a minicomputer or mainframe.

Network: A series of PCs connected in some type of topology (generally a star, ring or bus), using a special network operating system (NOS) that allows the PCs to share data and resources.

Local Area Network (LAN): A network that is set up for a department or limited geographic area. A peer-to-peer network shares resources with other PCs. A client/ server LAN can include midrange and legacy file servers and database servers.

Wide Area Network (WAN): A network that connects several networks in distant locations. The terms network, LAN, and WAN are synonymous with regard to applicability of the policies described herein.

(B) Job Descriptions

Network administrator

The duties of the network administrator shall include monitoring network efficiency (response time, utilization of disk space, etc.); troubleshooting network problems, monitoring environmental conditions; backing up the system, shared data files, and application programs on the file server; and preventing and detecting computer viruses.

Other duties include ensuring that network security features in the NOS are implemented,

recommending software and hardware acquisitions needed to maintain operating efficiency, contacting network maintenance contractors regarding technical problems, deleting and adding users, coordinating the installation of new network hardware and software, and maintaining an inventory of network hardware and software. The network administrator will report suspected security problems to the Nodal Officer/System Administrator/Uncharged Computer Centre and will coordinate with the security officer on producing security reports. The network security officer will address any security concerns identified by the report.

Network Security Officer

Duties of the network security officer include monitoring security violations on the network (unauthorized and unsuccessful access attempts), password administration, and any other duty deemed necessary by the Board or its committees to enhance the security of the network. Department should have its own Network Security Officer to perform above duties however, Network Security Officer could be arrange for maintenance of WAN.

(C) Compliance with Policy

The Heads of the department are responsible for ensuring that their employees comply with the policy. The IT Manager is responsible for reporting to the network administrator any support needs or concerns, except security. Security concerns will be communicated to the network security officer.

12.2 Network Security

This section discusses the types of security and security policy regarding access control, passwords, and data security in a networked environment.

(A) Types of Security

The Office's network has four types of security:

- Log in/Password (initial access)
- Trustee (directory level access)
- Directory (directory level access)
- File attributes (file level)

Log in/Password

Security is activated when a user logs in to the network. The server requires both a recognizable user name and a password. Each user chooses his or her own password, which is encrypted by the system. If the user forgets the password the network administrator must assign a new one.

Trustee

A trustee is a user who has been given rights to a directory and the files it contains. Trustee rights can be assigned to both individuals and groups. A trustee will not assign directory or file rights to a user who does not have a legitimate need to use that file or directory. Trustees will ensure that confidential office information to which they have access is not written to removable media and transported off Office premises unless authorized by the departmental supervisor or performed by authorized individuals as part of backup and emergency/recovery procedures. In addition, reports printed using the data should be distributed only to authorized users.

Directory

The directory security defines a user's rights in a given directory. These rights are:

- Supervisor (assigns the rights for the directory)
- Access control (trustee assignments)
- File scan (search)
- Modify filenames and attributes
- Create new files or subdirectories
- Erase existing files or subdirectories
- Read files
- Write files

The owner will not assign rights to users who do not have a legitimate need or authority to view or use the information.

File Attributes

The owner of a file has the right to set the following attributes:

- Shareable read only
- Shareable read write
- Non-shareable read only
- Non-shareable read write
- Hidden file
- Delete inhibit
- Rename inhibit

Assignment of these rights is designed to prevent accidental changes or deletions to the files. The owner of a file containing confidential information will not assign access to a user that does not have a legitimate need or authority to use the file.

(B) Network Security Policy

The objective of the Office's network security policy is to provide adequate IT controls over the network. Security features available on the network will be implemented as needed to restrict users to the resources and rights, necessary to perform all the duties of their job descriptions adequately. The network administrator, based on a written user setup form, from the departmental supervisor, showing password rights and normal work schedule, initially assigns rights. The rights may be expanded only with the written approval of the departmental supervisor.

Access Control

The network administrator will implement available security access control features of the network. These features include the ability to restrict:

- Files that a user can access
- Time periods that a user can log on to the network
- Days of the week that a user can log on to the network
- Workstations that a user can access

Once implemented, network access should be restricted to normal working hours whenever possible. Departmental supervisors can grant exceptions based on need or shift considerations. Adequate supervision and review of work are required for users who have access beyond normal working hours. Generally users should be allowed access only from pre-specified workstations (nodes).

Password

The network administrator sets up the user, and the user is required to enter a password on the first log on. Passwords will be set to expire every fifteen days. The system will be set to prompt the user for a password change automatically. Failure to make the change will cause the system to lock out the user. Also, repeated attempts to log on with an incorrect password will cause the intruder detection lockout to activate. The network software should not display the password on the screen. Users should not let anyone see their password as they are keying it in.

User passwords should have a minimum of six digits, with a mix of alphabetic and numeric characters. Users will not use passwords that can be easily guessed, such as family names, birthdays, and commonly used default passwords, such as "test," "password," or "demo." Users are not restricted by terminal, but are prohibited from logging on to more than one terminal at a time. Users are mainly subject to an inactive log off and automatic log off is not always available, users should manually log off when not using the terminal for that period of time or longer. When a user leaves the Office, the personnel department will notify the network administrator, who will deletethe user's password. Also, if a password is compromised, the user will change the password.

Data Security

Data should be saved to the appropriate directory, normally either the group directory or the departmental directory. In some cases, the supervisor authorizes the use of the user's local directory for storing certain types of data. Other members of the group access information on the group directory. Members of the department can access departmental directories. The user's local directory is on the PC and can be accessed only by the user.

User Responsibilities for Data Security

Users are responsible for backing up files on their individual PC hard drives, and departmental supervisors should verify that users are doing so on a regular basis. Users are also responsible for the security of their individual workstations, including security of PC backup disks.

Users are responsible for access security. Passwords should not be written down or seen by others when they are keyed in. Other related responsibilities include noting and reporting maintenance problems (such as disk error messages) before they can cause loss of data; ensuring that the PC data disks are not subjected to excessive heat, electrical fields, dirt, smoke, food particles, or spilled liquids; and ensuring that the PC has a surge protector.

(C) Monitoring the Network

Data Scope

A data scope is a device used to monitor network traffic. Its use, however, requires additional security controls to prevent abuse. Network Security Officer may have access of data scope to reduce any miss happening.

Performance Monitoring

Data integrity and security are enhanced when the system is running smoothly and is at peak performance. The network administrator should monitor performance of the system using available diagnostic tools. One of the duties of the network administrator is to troubleshoot any problems on the network and maintaining performance logs.

(D) Prevention and Detection of Viruses

The scheduler for the network's antivirus software will be set to scan memory and all files on the network on a daily basis. Warning messages will be carefully evaluated and corrective action taken. If a virus is discovered, the LAN security officer will investigate the origin of the virus. The policy for preventing viruses will be evaluated to determine the cause for the security failure. The security officer will recommend action to prevent future occurrences.

The origin of most viruses is "pirated" software or shareware or public domain software downloaded from a bulletin board, on-line service, or the Internet. All software will be scanned for viruses before being loaded on a PC.

The network administrator will purchase and install anti-virus software updates as they become available.

If the origin of the virus is due to negligence or policy violation on the part of an employee, that employee will be subject to appropriate disciplinary action, which may include termination.

12.3 Network Software

This section defines policies regarding:

(A) Software licensing violations
(B) Authorized software
(C) Personal use of Office software
(D) Ownership of software
(E) Custom development of software
(F) Support of purchased software

(A) Software Licensing Violations

All software installed on Office PCs and on the network will comply with the software's licensing agreement. Software licensed for a server is limited to the number of users covered by the license. An original disk must exist for each software application installed on a user's PC. The only exception is software with a site license or public domain software on an authorized list. In the case

of authorized shareware products, if the Office uses the software beyond the trial period, the author will be paid the suggested contribution. So-called "pirated" software will not be installed on Office PCs.

(B) Authorized Software

Only software, authorized by the Office may be installed on a network or on an individual PC. Users will not install personal software on a PC without the approval of their supervisor. No games or entertainment packages will be installed. The owner must show proof of ownership. An antivirus program will be run before installing any program on a PC. The Office will discourage the use of other than standard authorized software.

(C) Personal Use of Office Software

Users may NOT copy Office-owned software for their personal use, for distribution to others, or for use on another Office PC. Office software may be copied only for legitimate backup purposes.

(D) Ownership of Software

PC software developed by Office employees on Office-owned equipment and/ or during normal working hours is owned by the Office.

(E) Support of Purchased Software

The officer in charge (usually the network administrator) of the department that recommend LAN-based commercial software is responsible for completing and returning the product registration forms. A copy of the receipt and product identification number (usually the serial number) should be recorded for reference when making support calls.

Officer in charge or IT matters or Nodal Officer (IT) of user departments as may be authorized by the HOD should note (from the box or software license information) the support period expiration and coordinate with users to ensure that calls are made before expiration of the service period.

For other than off-the-shelf LAN software, the Office will obtain a written agreement detailing terms of maintenance support. The contract will clearly define hardware maintenance services and costs.

13 NETWORK HARDWARE

This section will discuss the Office's policy regarding the following:

(A) User responsibilities for hardware
(B) Hardware maintenance
(C) Integration with other systems
(D) Modems

(A) User Responsibilities for Hardware

Hardware refers to the physical components of the LAN-the PC workstations, monitors, peripheral equipment, routers, modems, etc. Users are responsible for taking reasonable care of the system and reporting to a supervisor any maintenance problems, particularly disk errors or other problems that might cause loss of data. Users may not remove hardware from the Office or transfer equipment to other locations in the Office without supervisory approval.

- Users should avoid subjecting PCs to excessive vibration or bumps. Hard jolts while a PC is running can damage the hard disk drive. Smoke, heat, magnetic fields, and excessive dust can also damage LAN equipment. All PCs should have a surge protector.
- Users should use good judgment when eating or drinking in the vicinity of PCs and LAN equipment.
- The network administrator should locate the server in a secure area.

(B) Hardware Maintenance

The network administrator may, from time to time, get into annual maintenance agreements for selected equipment as deemed necessary. The network administrator will have emergency phone numbers and contract sources available it is necessary to replace or repair critical network components quickly.

(C) System Integration

Users can utilize PCs as terminals connected to a mainframe as well as workstations connected to a network. Data moves back and forth between the network and other systems, using the open standard protocol.

(D) Modems

The Office uses modems for communication with selected departments, clients, and employees. Modems will be turned off when not in use. The network administrator will activate applicable security features that are available. The senior management will approve modem controls. The following modem controls should be implemented if permitted by hardware and software:

- Limitation of the activities that can be performed
- Auto call back to identify dial-in users
- Passwords
- Unique operator identification
- Automatic log-off after a predetermined number of failed access attempts

14 LAN BACKUP AND RECOVERY POLICIES

The network administrator will identify critical and/or sensitive network data files and applications and ensure that these are adequately protected and backed up. The network administrator is responsible for backup at the Office's data center. The responsibility for backing up

at branches lies with the assistant network administrators.

14.1 LAN Purchasing Policy IT Steering Committee

Every department should have an IT steering committee headed by the HOD. It is the responsibility of the IT steering committee to develop long-term and short-term plans for purchasing LAN hardware and software. The committee has the responsibility to initiate requests for major purchases. The network administrator is responsible for purchasing the approved equipment and software after observing required formalities.

15 ROLE OF SYSTEM ADMINISTRATOR IN VIRUS PROTECTION

15.1 Computer Viruses: Detection and Removal Methods

(A) Anti-Virus Programs
(B) Detection of an Unknown Virus
(C) Prophylaxis of Computer Infection
(D) Recovery of Affected Objects

(A) Antivirus Programs

Anti-virus programs are the most effective means of fighting viruses. But there are no antivirus guaranteeing 100 present protections from viruses. Comprehensive software like Norton Internet Security and McAfee Active Virus Defense (AVD) are the easiest way to combat most computer security troubles. Such software provides essential protection from viruses, hackers and other privacy threats. It is necessary to pay attention to some terms as following, used in anti-virus program discussion:

- **False Positive -** when an uninfected object (file, sector or system memory) triggers the anti-virus program. The opposite term - False Negative – means that an infected object arrived undetected.
- **On-demand Scanning** - a virus scan starts upon user request. In this mode, the anti-virus program remains inactive until a user invokes it from a command line, batch file or system scheduler.
- **On-the-fly Scanning** - all the objects that are processed in any way (opened, closed, created, read from or written to etc.) are being constantly checked for viruses. In this mode, the anti- virus program is always active. It is a memory resident and checks objects without user request.

Which Anti-Virus Program is better?

Which anti-virus program is the best? The answer is any program, if no viruses live in the computer and user uses only a reliable virus-free software source and no other. However, if user likes using new software or games, active e-mail user, likes using Word or exchanging Excel spread sheets, then one should use some kind of anti-virus protection. Which one exactly - should be decided on his/her own, but there are several points of comparison of different anti-virus programs. The following points, from the most to least importance, determine the quality of anti-virus programs:

- Reliability and convenience of work
- Detection of all major kinds of viruses- scanning inside document files, spread

sheets
(Microsoft Word, Excel), packed and archived files.

- Ability to cure infected objects.
- Availability of timely updates, which is the speed of tuning a scanner to new viruses.
- Availability of anti-virus versions for all the popular platforms (Windows, Windows NT, Novell NetWare, OS/2, Alpha, Linux etc.)
- Availability not only on-demand scanning, but also scanning on-the-fly capabilities, availability of server versions with possibility for network administration.
- Speed of work and other useful features, functions, bells and whistles.

Reliability of anti-virus programs is the most important criterion, because even the "absolute anti-virus" may become useless, if it is not able to finish the scanning process and hangs. It will leave a portion of the disks and files unchecked, thereby leaving the virus in the system undetected. The anti-virus may also be useless if it demands some special knowledge from a user - most users are likely to simply ignore the anti-virus messages and press [OK] or [Cancel] at random, depending on which button is closer to the mouse cursor at this time. And if the anti-virus asks an ordinary user complicated questions too often, the user will most likely stop running such an anti-virus and even delete it from the disk.

Tips on Usage of Anti-Virus Programs

- Always see that the latest antiviral software version available. If software updates are available, check them for "freshness".
- If a virus has been found on the computer, it is imperative not to panic (for those who "meet" viruses daily, a remark like this may seem funny). Panicking never does any good; thoughtless actions may result in bitter consequences.
- If a virus is found in some newly arrived file(s) and has not infiltrated the system yet, there is no reason to worry: just kill the file (or remove the virus with antivirus program) and keep on working. If virus is found in several files at once or in the boot sector, the problem becomes more serious, but still it can be resolved.
- In the case of file-virus detection, if the computer is connected to a network, disconnect it from the network and inform the system administrator. If the virus has not yet infiltrated the network, this will protect the server and other workstations from virus attack.
- If the virus has already infected the server, disconnection from the network will not stop the virus from infiltrating into the computer again after its treatment. Reconnection to the network must be done only after all the servers and workstations have been cured.
- If a boot virus has been found, don't disconnect the computer from the network; viruses of this kind do not spread over it (except file-boot viruses).
- If the computer is infected with a macro-virus, then instead of disconnecting from network, it is enough to make sure that the corresponding editor (Word/Excel) is inactive on any computer.
- If a file or boot virus has been detected, make sure that either the virus is non-resident, or the resident part of it has been disarmed: when started, some (but not all) anti-viruses automatically disable resident viruses in memory. Removal of a virus from the memory is necessary to stop its spreading. When scanning files, anti-viruses open them; many resident viruses intercept this event and infect the files being opened. As a result, the majority is infected because the virus has not been removed from memory yet. The same thing may

happen in the case of boot viruses - all the diskettes being checked may become infected. If the anti-virus used, does not remove viruses from memory, reboot the computer from a known uninfected and well-written, protected system diskette. User should do a "cold" boot (by pressing "Reset" or power "off/on"), because several viruses "survive" after a "warm" boot. Some viruses apply a technique allowing for their survival even after the "cold" boot.

- With the help of the anti-virus program, restore the infected files and check them for functionality. At the same time or before treatment, backup the infected files and print/save the anti-virus log somewhere. This is necessary for restoring files in case the treatment proves to be unsuccessful due to an error in anti-virus-treatment module, or because of an inability of this anti-virus to cure this kind of virus. In this case, resort to the services of some other antivirus.
- It is much more reliable, of course, to simply restore the backed up files (if available), but, still, resort to an anti-virus - what if all the copies of the virus haven't been destroyed, or some backed up files are infected, too?
- It is worth mentioning that the quality of file restoration by many antivirus programs leaves much to be desired. Many popular anti- viruses often irreversibly damage files instead of curing them. Therefore, if file loss undesirable, execute all the previous recommendations completely.
- In the case of a boot virus, it is necessary to check all the diskettes to see whether they are bootable (i.e., contain DOS files) or not. Even a completely blank diskette may become a source of viral infection - it is enough to forget it in the drive and reboot (of course, if a diskette boot is enabled in BIOS).
- Colonies of viruses may infiltrate backup copies of software, too. Moreover, archives and back-up copies are the main source of long known viruses. A virus may "sit" in a distribution copy of some software for ages and then suddenly appear after software installation on a new computer. Nobody can guarantee removal of all copies of a computer virus, because a file virus may attack not only executable, but also overlay modules not having COM or EXE extensions. A boot virus may remain on some diskettes and appear suddenly after an attempt to boot from it. Therefore, it is sensible to use some resident anti-virus scanner continuously for some time after virus removal (not to mention that it's better to a use scanner at all times).

(B) Detection of an Unknown Virus

Detection of a TSR Virus

- DOS Viruses: If traces of virus activity have been found in a computer, but no visible changes in the file or system sectors of discs can be found, then it is quite possible that the computer is infected by one of the Stealth viruses. In this case, it is necessary to boot from DOS using a verified virus free diskette with a backup copy of the DOS, and do the same as in the case of non-resident viral infection. However, sometimes this is undesirable, and in a few cases even impossible, for example, there is known cases of the purchase of new computers, which have already been infected by a virus. Then detect and neutralize the resident part of the virus with the use of Stealth technology. There are several ways to look in to the memory for the virus or for its resident part of infecting memory.
- Windows Viruses: Detection of a resident Windows virus is an extremely difficult task. A virus in the Windows environment as an application or as a VxD driver is virtually invisible

because of several more dozens of active applications and VxDs not unlike the virus in their external display. To detect the virus program in an active applications list or VxD list, it is imperative to have extensive knowledge of the "internals" of Windows and have complete information about applications and drivers installed in this particular computer. Therefore, the only suitable way of catching a resident Windows virus is to boot up DOS and check the Windows executable files with the help of the methods described above.

Detection of a Boot Virus

As a rule, boot sectors of disks carry small programs, whose purpose is to determine borders and sizes of logical disks (for MBR (Master Boot Record) of hard drives) or operating system boot up (for boot sector).

In the beginning, user should read the contents of the sector suspected of virus presence. DISKEDIT from Norton Utilities or AVPUTIL from AVP Pro are best suited for that.

Some boot viruses may be detected almost immediately by the presence of various text strings (for example, the "Stoned" virus contains the strings: "Your PC is now stoned! “LEGALISE MARIJUANA!"). Some boot viruses infecting hard disks may be found in the opposite way, by the absence of strings, which must be in the boot sector. Such strings are: system file names (for example, "IO SYSMSDOS SYS") and error message strings. Absence of or change in a header string of the boot sector (the string containing the DOS version number or software vendor name, e.g., "MSDOS5.0" or "MSWIN4.0") may also be a signal of viral infection, but only if the computer does not have Windows98/NT installed, these systems, for reasons unknown, record random text string into a diskette’s boot sector header.

Standard MS-DOS loader located in MBR occupies less than half a sector and many viruses infecting the MBR of a hard drive are easily spotted by an increase in the size of the code in MBR sector.

However, there are viruses, which infiltrate the loader without changing its text strings and with minimum changes to the loader code. To detect such a virus, in most cases, it is sufficient to format a diskette on a 100% uninfected computer, save its boot sector as a file, use this diskette for some time on the infected computer (read/write several files) and afterwards compare its current boot sector with the original one on an uninfected computer. If the boot code underwent some changes, then the virus has been caught.

Detection of a File Virus

- As already mentioned, viruses are divided into resident and non-resident. Resident viruses found so far stood out for their much greater craftiness and sophistication in comparison with non-resident. Therefore, we shall discuss the simplest case for starters - attack of an unknown non-resident virus. Such a virus activates itself upon starting of any infected programs, does all it has to, passes control to the host program and afterwards (unlike resident viruses) does not interfere with its work. To detect such a virus, it is necessary to compare file size on disks and in backup copies. If this doesn’t help, do a byte comparison of distribution copies with the working copies. At the present, there are many such programs; the simplest of them (COMP utility) can be found in DOS.
- One may also examine a hex dump of executable. In some cases, it is possible to immediately detect viral presence by some text strings residing in its code. For example, many viruses contain strings ". COM", .*.COM", ..EXE", "*.EXE", "*.*", "MZ", "COMMAND"

etc. These strings may often be found at the top or end of the infected files.

- There is yet one more method for the visual detection of a virus in a DOS file. It is based on the fact that executable, the source code of which was in a high level programming language, have a quite definite inside structure. In the case of Borland or Microsoft C/C++ program, the code segment is at the very beginning of a file, immediately followed by the data segment containing a copyright notice with the name of a compiler vendor company at the beginning. If the data segment in the dump is followed by one more code segment, then it might very well be that the file is infected with a virus. The same is true for the most part of the viruses, whose target is Windows and OS/2 files. In these, OS executable has the following standard order of segments: code segment(s) followed by data segments. If a data segment is followed by one more code segment, it may be the sign of the presence of a virus.

The above methods of detection of file and boot viruses are suitable for most resident and non-resident viruses.

Detection of a Macro Virus

Characteristic features of macro-viruses are:

- Word: inability to convert an infected Word document to another format.
- Word: infected files have the Template format, because when infecting, Word viruses convert files from the Word Document format to Template format.
- Word 6 only: inability to save a document to another directory or disk with the "Save As" command.
- Excel/Word: "alien" files are present in the STARTUP directory
- Excel versions 5 and 7: Cookbooks contain redundant and hidden Sheets.

To check the system for viral presence, the Tools/Macro menu item can be used. If "alien" macros have been found, they may belong to a virus, but this method fails in the case of Stealth viruses, which disable this menu item, which in itself is sufficient to consider the system infected.

Changes in Word, Excel and Windows system configuration files are also a sign of possible infection. Many viruses change menu items under "Tools/Options" in oneway or another - enabling or disabling the following functions: "Prompt To Save Normal Template," "Allow Fast Save," "Virus Protection." Some viruses set file passwords after infecting them, and a lot of viruses create new sections and/or options in the Windows configuration file (WIN.INI).

Of course, such obvious facts such as appearing messages or dialogues with strange contents or in a language other than the default for this installation are also signs of virus.

(C) Prophylaxis of Computer Infection

- Where do Viruses come from
- The main rules of protection
- The problem of Macro Virus Protection
- Macro Virus Protection for Office XP

One of the major methods of fighting computer viruses, like in medical science, is timely prophylaxis or preventive measures. Computer preventive measures suggest following a small set of rules, allowing lowering considerably the possibility of virus infection and data loss.

To define the main rules of computer hygiene, it is necessary to find out the main ways of virus intrusion into computer and computer network.

Where do Viruses Come From

- Global Access Networks and Email
- Email Conferences, File Servers, FTP and BBS
- Local Access Networks
- Pirated Software
- General Access Personal Computers
- Repair Services

The Main Rules of Protection

- Rule 1:
  Be very careful with programs and documents of Word/Excel received from global access networks. Before executing a file or opening a document/spread sheet/database be sure to check them for viruses. Use customized anti-viruses to check the entire file coming via email and Internet on the fly.

- Rule 2:
  To lower the risk of infecting files on the server network administrators have to make extensive use of standard network security features: user access restrictions; setting "read-only" or even "execute only" attributes for all that executable (unfortunately this may not always be possible) etc. Use customized anti-viruses, checking the files in use on the fly. If for some reason this is impossible, run conventional anti-virus programs on server disks regularly. The risk of computer network infection becomes considerably lower in case of use of diskless workstations. It is a good idea before running some new software on the network to test it on a stand-alone trial computer, not connected to network.

- Rule 3:
  It is better to buy software distribution packages from official vendors, instead of having free copy from other sources or buying pirated copies. This way the risk of infection is considerably lower, although there are known cases of purchase of infected distribution packages. As a consequence from this rule goes the necessity of keeping distribution copies of software (including copies of operating system), and preferably on write-protected diskettes. Also use only well-established source of software and other files, although this is not always helpful (for example for a long time on the Microsoft WWW server there has been a document infected with "Wazzu" macro virus). Apparently the only reliable sites from the point of view of virus protection are BBS/ftp/WWW sites of anti-virus development companies.
- Rule 4:
  Try not to run unchecked files including those received via computer network. Use only those programs received from reliable source. Before running the programs be sure to check them by one or several anti-virus programs.

Even if none of the anti-virus programs triggered by the file, downloaded from a BBS or newsgroup, don't hurry to run it. Wait for a week; it is possible that this file is infected with some new unknown virus, in that case somebody else might "step into it" before informing about it.
It is also desirable to have some kind of a resident anti-virus monitor when working with some new software. If virus infects executed program, such a monitor will have to detect virus and prevent it from spreading.
All this leads to necessity of limiting of a number of persons using a particular computer. Multi-user personal computers are generally most prone to infection.

- Rule 5:
  Use validation and data integrity checking utilities. Such utilities like the special databases of disks system areas (or keep the entire system areas in databases) and file information (check sums, sizes, attributes, last modification dates etc.). Periodically compare such database information with actual hard drive contents, because any inconsistency might be a signal of presence of a Trojan horse or virus.

- Rule 6:
  Back-up working files periodically. The expenses of backups of all source code files, database files, document files etc. are much lower than the expenses of restoring these files in case of a virus attack or a computer malfunction. If department have a streamer or other mass storage device, then it makes sense to back up all the hard drive's contents. The duty and the fact that such a backup copy needs a lot of time to be the created; it makes sense to make such backups less often.

- Other Rules:
  If there is no need to boot the system from a floppy drive every day, set the boot order in BIOS Setup as "C: A:" This will protect computer from boot viruses reliably. Do not rely on the built-in BIOS virus protection; many viruses pass it by with the help of different techniques. The same goes for anti-virus protection, which is built into Word and MS-Office. This protection can also be disabled by virus or by user (because it may be a nuisance).

The Problem of Macro Virus Protection

Due to the fact that the macro virus problem nowadays exceeds all the other virus related problems, it is worth of a more detailed explanation.

There are several techniques and a number of built-in Word and MS-Office functions aimed at prevention of executing a virus. The most efficient of them is Word and Excel (starting from versions
7.0 a) built in virus protection. When opening the file containing any macro, this protection informs about its presence, and suggests disabling this macro. As a result the macro is not only disabled but also cannot be seen by means of Word/Excel.

Such a protection is rather reliable, but absolutely useless, if user works with macros of any kind: it does not make difference between virus macros and non-virus macros and displays the warning message before opening virtually any file. For this reason the protection becomes disabled in most cases, which gives viruses opportunity to infiltrate the system. Besides that activating virus protection in an already infected system not always helps -some viruses, once taken control, with each execution disable virus protection feature and therefore completely block it.

There are other virus counter measures, for example the Disable Auto Macros function, however it does not prohibit execution of other macros and blocks only those viruses, which use one of the auto macros for their propagation.

Executing Word with /M option (or with pressed Shift key) these tables only the AutoExec macro and therefore cannot be a reliable virus protection feature.

Macro Virus Protection For Office XP

One can configure Office XP to protect users against macro viruses on several fronts, starting with setting macro security protection levels in the Options dialog of each Office application.

These configuration options determine what happens when a user opens a document. For example, if your department security policy requires digital signatures, you might automatically disable macros that aren't signed. That way, only macros created within your user community and by legitimate software companies will run.

We can use security levels to set macro security on most Office XP applications. The Custom Installation Wizard and Custom Maintenance Wizard, along with the Office Profile Wizard, System Policy Editor, and Windows 2000 Group Policies all provide with valuable tools to help enhance macro virus protection.

The following macro security settings are available:

High: Only signed macros from trusted sources are allowed to run. Unsigned macros are automatically disabled.

Medium: The user can choose whether to run potentially unsafe macros. When a user opens a document that contains macros, he or she is asked to confirm whether the macros should run.

Low: All macros run without any security warnings.

In addition, Microsoft Outlook® version 2002 provides a robust set of protective devices that help you avoid macro viruses delivered as e-mail attachments.

By default, Outlook blocks executable file type attachments, such as .bat, .exe, .com, .vbs, and .js. Other file types can be saved to a user's hard drive, but cannot be executed within Outlook. If a program tries to access the Outlook address book, a warning dialog appears, giving the user the option to allow or prevent access.

(D) Recovery of Affected Objects

- Recovery of Word Document and Excel Spread sheets
- Boot Sector Recovery
- File Recovery
- RAM deactivation

In most cases of virus infection the procedure of recovery infected files and disks means running a

suitable anti-virus capable to disinfect the system. However, if any anti-virus does not know the virus, it is enough to send the infected file to anti-virus developer companies.

Recovery of Word Document and Excel Spread sheets

To disinfect Word and Excel it is enough to save all the necessary information in no document and non-spread sheet format - RTF text format is most suitable for this purpose, it contains virtually all the information from original documents but does not contain macros. Then exit Word/Excel, delete all the infected Word documents, Excel spread sheets and all the documents/spread sheets in start-up directories of Word/Excel. After that run Word/Excel and recover documents/spread sheets from RTF files.

As a result of this procedure, the virus will be deleted from system, and all the information will remain virtually unchanged. But this method has its own disadvantages. The main one is that the process of converting documents and spread sheets to RTF format and back might be very time-consuming for large number of files. Besides that in case of Excel it is necessary to convert each sheet in each Excel file separately. Another drawback is the loss of all non-virus macros used in work. Therefore before beginning the described procedure one should save their source text, and after disarming the virus restore the necessary macros in their original form.

Boot Sector Recovery

Boot sector recovery in most cases is rather simple and can be done with the help of DOS SYS
command (for boot sectors of diskettes and logical disks of hard drives) or with the help of the FDISK /MBR command (Master Boot Record of hard drives). Of course one might use the FORMAT command, but virtually in all cases SYS will do. One should keep in mind that sector recovery must be done only under the condition of absence of virus in RAM. If RAM copy of virus has not been disarmed, then it is quite possible, that the virus will repeatedly infect diskette or hard drive after the removal of viral code (even if after using the FORMAT utility).

Also **be very careful while using FDISK/MBR**. This command rewrites completely the code of the system loader routine and does not change the Disk Partition Table. FDISK/MBR is a 100 percent successful cure for most boot viruses, however, if the virus encrypts the Disk Partition Table or uses nonstandard methods of infection, FDISK/MBR may result in complete loss of information on disk. Therefore before running FDISK/MBR, make sure that the Disk Partition Table is intact. To do so, boot to DOS from an uninfected diskette and check the validity of this Table. (Norton Disk Editor could be used the purpose).

But if sector recovery with the help of SYS/FDISK is impossible, usually figure out the operating algorithm of the virus, find the original boot/MBR sector on disk and move it to the proper place (Norton Disk Editor or AVPUTIL could be used for the purpose). Doing that constantly keep in mind that when rewriting system loaders user must be extra careful, because incorrect adjustment of the MBR or boot sector may result in total loss of all the information on disk(s).

File Recovery

In the vast, majority of cases recovery of infected files is complicated enough. This procedure is impossible to be carried out without the necessary knowledge of executable file formats, assembly language, etc. Besides that usually several dozens or hundreds of files become infected at once, and

to disarm them it is necessary to create an anti-virus program of your own or contact antivirus developing company.

When curing files consider the following rules:

- It is necessary to test and cure all the executable files (COM, EXE, SYS, overlays) in all the directories of all disks irrespective of file attributes (that is read-only, system and hidden);
- It is desirable to keep file attributes and the date of last modification unchanged;
- The possibility of multiple infections of one file must be regarded.

The treatment of the file itself in most cases is carried out by one of several standard methods, depending on the algorithm of multiplication of virus. In most cases file header recovery and size adjustments do the job.

RAM deactivation

The RAM deactivation procedure, like treatment of infected files, requires some knowledge of OS and assembly language expertise.

While treating RAM it is necessary to detect where the virus goes and change them in such a way that the virus could not prevent the anti-virus program from working further - "disable" the infection and Stealth routines. To do this it is required to have a complete analysis of the virus code done, because the infection and Stealth routines may be situated in different areas of the virus, duplicate each other and take control under different circumstances.

When deactivating a TSR copy of the virus, it is imperative to remember, that the virus might take special precautions for recovery of its own code (for example, some viruses of the "Yankee" family restore themselves using the method of error-correcting encoding), and in this case the mechanism of self-recovery of the virus must also be neutralized. Besides that several viruses calculate the CRC of their resident copy and reboot the computer or erase disk sectors, if the calculated CRC differs from the original value. In this case the CRC calculation routine must also be "disarmed".

15.2 Computer Virus Classification

Viruses can be divided into classes according to the following characteristics:

- Environment
- Operating system (OS)
- Different algorithms of work
- Destructive capabilities

Do not forget that there also exist other "harmful" programs or so-called "malware" such as Trojan horses.

ENVIRONMENT: According to the ENVIRONMENT, viruses can be divided into the following:

- File: - either infect executable in various ways (parasitic - the most common type of viruses), or create file doubles (companion viruses), or use file-system specific features (link viruses).
- Boot Viruses: - either saves itself in a disk boot sector or to the Master Boot Record, or change the pointer to an active boot sector.
- Macro: - infect document files, electronic spread sheets and databases of several popular software packages.
- Network: - use protocols and commands of a computer network or e-mail to spread Themselves.

There exists a large number of combinations; for example, file-boot viruses infecting both files and boot sectors on disks. Another example of a combination is a network macro-virus, which not only infects documents being edited, but also sends copies of itself by e-mail.

OPERATING SYSTEM: The target operating system (namely the OS specific objects prone to attack) is the second level of division of viruses into classes. Each file or network virus infects the files of one particular or several OS - DOS, Windows 3.xx, Windows95/NT, OS/2 etc. Macro-viruses infect Word, Excel, and MS-Office format files. Boot viruses are also format oriented, each attacking one particular system-data format in disk boot sectors.

OPERATING ALGORITHMS: Among OPERATING ALGORITHMS the following features stand out:

- TSR Capability: - A TSR virus, while infecting a computer, leaves its resident part in the RAM, which then intercepts system calls to target objects and incorporates into them. Resident viruses reside in memory and are active until power down or until operating system reboot. Non-resident viruses do not infect computer memory, and are active for a limited time only. Some viruses leave small resident parts in the RAM, which do not spread the virus. Such viruses are considered non-resident.
- Macro-viruses can also be considered residents, because they reside in the computer memory during the entire running time of the infected editor program. Here the editor plays the role of the operating system, and "system reboot" means editor program termination.

- In multitasking operating systems, the lifetime of a resident DOS virus can also be limited by the moment of closing the infected DOS window, and the activity of boot viruses in some operating systems is limited to the moment of OS disk drive installation.

- Stealth Algorithms: - The use of Stealth algorithms allows viruses to completely or partially cover their tracks inside the OS. The most common stealth algorithm is the interception of OS read/write calls to infected objects. In such cases, stealth viruses either temporarily cure them or “substitute” themselves with uninfected pieces of information. In the case of macro-viruses, the most popular technique is to disable the View Macro menu(s). "Frodo" is one of the first file Stealth viruses; "Brain" is the first boot Stealth virus.

- Self-Encryption and Polymorphic Capability: - These capabilities are used by virtually all types of viruses to make the virus detection procedure as complicated as possible. Polymorphic viruses are really hard to detect; they have no signatures; that is, none of their code fragments remain unchanged. In most cases, two samples of the polymorphic virus will not have a single match when doing a byte comparison. This may be achieved by encrypting of the main body of the virus and making modifications to the decryption routine.

- Use of Non-Standard Techniques: - A variety of Non Standard Techniques are used in viruses to hide themselves as deep as possible in the OS kernel (as in "3APA3A"), to protect its resident copy from being detected and makes curing more difficult (for example placing its copy into Flash BIOS) etc.

DESTRUCTIVE CAPABILITIES: Based on their DESTRUCTIVE CAPABILITIES, viruses can be divided as follows:

- Harmless, that is, having no effect on computing (except for the lowering of some free disk space as a result of propagation);
- Not dangerous, limiting their effects to the lowering of free disk space.
- Dangerous viruses, which may seriously disrupt a computer's operation;
- Very dangerous, the operating algorithms of which intentionally contain routines that may lead to loss of data, data destruction, erasure of vital information in system areas, and even, according to one of the unconfirmed computer legends, inflict damage to the moving mechanical parts by causing resonance in some types of HDDs.

But even if no destructive branches can be found in the algorithm of a virus, one cannot be perfectly sure that this virus is harmless, because its infiltration into a computer may prove to be unpredictable and sometimes have catastrophic consequences. This is due to the fact that any virus, like any program, may contain errors, which may damage both files and disk sectors.

15.3 Recommendation for Antivirus Software usage

- Workstations should have running the latest version of antivirus software, scanning engine and the virus signature file.
- Virus definition should be upgraded regularly.

16 RECOMMENDATIONS FOR SYSTEM ADMINISTRATOR

- IT security policies, standards and processes should be made available to users in an easily accessible location.
- Security related duties should have a place in evaluations.
- Staff should be instructed on basic workstation security.
- There should be redundant hardware to allow work to continue in the event of a single hardware failure.
- They should be tested on regular interval.
- UPS should notify someone when it goes into operation and also should be tested on regular interval.
- There should be plans to have departmental hardware replaced at regular intervals.
- Department should have system maintenance standards and procedures.
- System Administrator/Nodal officer should ensure that all sensitive data is removed from equipment before being sent out for repair or replacement.
- Department should have original disks to reinstall the software if the hard drive fails.
- Department should have proper plans for old or unsupported software to replace it.

- Developer who developed local Software should be in easy reach to get support.
- Department should have provisions to continue operation if central services software is not available.
- All workstations cases should be locked to prevent access to internal components.
- Unused computers and peripherals should be kept in locked storage areas.
- Department should have a standard and procedure for sanitizing and disposing of confidential and sensitive material on hard drives, tapes, floppy disks, CDs, etc.
- Systems changes should be recorded.
- There should be a process for communication of systems changes.
- Department should have a version control plan for software products.
- Maintenance Records should be kept to indicate what repairs and/or diagnostics were performed and by whom.
- Department should maintain antivirus software and its updates for new virus definition.
- Department should have process of imparting computer training periodically.
- Department should have its backup policy and maintain its backup regularly.

- Department should have a policy for maintaining strong password.

17 SECURITY POLICY FOR DBA

'DBA' is a highly technical person who has specialized in the development and maintenance of database and database applications.

"The DBA is responsible for ensuring that all housekeeping routines are performed on the database, which may include designing and maintaining the structure and content of the (many) tables which together form the database, and the relationships between these tables. In addition, the DBA will usually be specialized in writing reports and querying the database, usually using Structured Query Language or SQL"

DBA is responsible for the development, maintenance, and integrity of databases as specified by the database owner.

DBA's Responsibilities includes

- Application Security.
- Access to Program/Database Objects.
- Access to Data in Database Tables.
- Access to application programs, reports, and queries.
- Access to ad hoc reporting tools.
- Installation, configuration and upgrading of database server software and related products.
- Evaluate database features and its related products.
- Establish and maintain sound backup and recovery policies and procedures.
- Take care of the Database design and implementation.
- Implement and maintain database security (create and maintain users and roles, assign privileges).
- Perform database tuning and performance monitoring.
- Perform application tuning and performance monitoring
- Setup and maintain documentation and standards.
- Plan growth and changes (capacity planning).

- Work as part of a team and provide 7x24 support when required
- Perform general technical trouble shooting and give consultation to development teams
- Designing, developing, organizing, managing, and controlling the database in accordance with security policies
- Providing the security access administration function with the necessary information to maintain user Ids and privileges; and, recovering database in a secure manner.

17.1 Policy on Transferring and Exchanging Data

"Sensitive or confidential data / information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured e.g. by using encryption techniques."

Data should be transfer or exchange through networks (both public and private) or through other means e.g. disks, diskettes and optical disks (e.g. CD-ROMs). Tapes or disks should be properly tagged.

Information Security issues to be considered then implementing policy includes the following:

- Incorrect data released to outside parties can lead to a loss of confidence in the organization and / or its services.
- Any illegal amendment of / tempering with the data whilst in transit suggests a weakness that is being exploited by techno-criminals / hackers.
- Where security measures have not been adequately deployed, sensitive information may be accessed by unauthorized persons
- Confidential data may be distributed to inappropriate / unauthorized persons.
- The recipient of the data may have adopted Information Security standards, which are incompatible with the department policy. This constitutes a weak link in the security, which could be exploited.
- The inappropriate and possibly illegal release of information may result in legal action and prosecution.

18 POLICY ON MANAGING DATA STORAGE

"Day-to-day data storage must ensure that current data is readily available to authorized users and that archives are both created and accessible in case of need."

The storage of information and data is a day-to-day function for all organizations. It requires careful management to ensure that Information Security issues are dealt with adequately.

Information Security issues to be considered when implementing your policy include the following:

- Where data and information files are not saved and stored securely, your organizations activities can be severely disrupted.
- important data may become unavailable due to deletion. This can lead to a range of difficulties, the least of which may be embarrassment.

18.1 Policy on Managing Databases

"The integrity and stability of the organization's databases must be maintained at all times."

The majority of your organization's data, such as client records, accounting data, project information, sales, and purchases, are likely to be held in databases of some form. Some databases will require active management, e.g. 'relational databases which comprise multiple tables of data.

Information Security issues to be considered when implementing your policy include the following:

- A failure to manage the technical requirements of the database can result in failure of the database itself and the applications which access and update it.
- Unless the data is periodically cleansed, its integrity will diminish as duplications and ambiguous records persist.

18.2 Policy on Permitting Emergency Data Amendment

"Emergency data amendments may only be used in extreme Circumstances and only in accordance with emergency amendment Procedures."

Sometimes referred to as 'data surgery', these measures are adopted when live data must be altered by other than normal software functions and procedures. This can occur when, for example, 'the system' will not permit the change to a data field on a 'confirmed' transaction - and yet the data is incorrect. Such manipulation of data is dangerous and can have knock-on effects, but occasionally it is necessary. Proceed with extreme caution. These amendments should be done with proper log involvement of senior management and should be used sparingly.

Information Security issues to be considered when implementing your policy include the following:

- Emergency data amendment can bypass your normal controls with the consequent scope for fraud and error.
- Unless rigorous procedures are implemented to control emergency data amendments; files may become corrupted or manipulated.

18.3 Policy on Setting up New Databases

"Databases must be fully tested for workflow logic and processing, prior to operational usage. Where such databases are to contain information of a personal nature, procedures and access controls must ensure compliance with necessary legislation e.g. Data Protection."

Databases are set-up so that specific data can be stored, retrieved and reorganized. This makes the maintenance of security and integrity of the data particularly important.

Information Security issues to be considered when implementing your policy include the following:

- Without a careful and diligent testing of a database, it's processing and reporting may be false, which could lead to inappropriate business decisions.
- New databases may be set up without proper consideration as to their data content and the appropriate storage and access control to apply to the data.

18.4 **Security Policy for Database**

"The DBMS features that provide for security and integrity are Encryption, Views, Authorizations, and User-defined procedures "

Data base security is generally classified under 3 headings:

Physical security	Protection against natural disaster, fire, flood, theft, malicious damage etc.
Operational security	Integrity, guarantee or protection (i.e. ensuring data is error free) and Reliability (i.e. ensuring the maintenance of a correct and whole database).
Authorization security	Ensuring the confidentiality of the data base for both private and legal reasons

Physical Security

- Locate installation in geographically inert places, if possible.
- Install fire control mechanisms.
- Use of security locks, access and exit to installation through fixed monitoring points will minimize theft and damage risks.
- Secure external doors, windows, walls etc., or better locate the installation in the center of a building

. Operational

Security

Protecting the integrity of the database, i.e. ensuring that the things users do are correct.

The integrity of a database is measured by the rules, which it must obey. Any given operation (an access, update, deletion etc.) is invalid if it violates the rules. Many of the integrity constraints (rules) are associated with checking data items, e.g.:

- Correct domain for an attribute
- Type checking
- Limit checking

Other constraints might be concerned with records are as

- Cannot delete the associated record if there exists one to many relationship.
- Authorization Security

The most important responsibility of administrator is to secure data. Securing database involves:

- Preventing unauthorized access to classified data.
- Preventing service engineer to access the data.
- Monitoring user access of data through auditing techniques.
- Use encryption techniques so that data is stored in 'coded' form. Anyone accessing the data needs to decrypt the data.
- Implement views with to limit access of users to those areas of the database that are permissible.
- Use program authorization and passwords. Passwords can be applied at all levels.
- Apply authorization rules:
- Subject - WHO
- Object - WHAT
- Action - HOW
- Constraint – LIMIT

18.5 Guidelines/Recommendation for DBA

- To Create and maintain all databases required for development, testing, Education and production usage.
- To perform the capacity planning required for creating and maintaining the databases. The DBA works closely with system administration staff because computers often have applications or tools on them in addition to the Databases.
- To Performs on-going tuning of the database instances.
- To install new versions of the Databases and its tools and any other tools that access the database.
- To Plan and implement backup and recovery of the database.
- To Control migrations of programs, database changes, reference data changes and menu changes through the development life cycle.
- To Implement and enforce security for all of the Databases.
- To perform database re-organizations as required assisting performance and ensuring maximum uptime of the database.
- To ensure that all applications design and code is produced with proper Integrity, security and performance. The DBA will perform reviews on the design and code frequently to ensure the site standards are being adhered to.
- To Evaluate releases of new database and its tools, and third party products to ensure that the site is running the products that are most appropriate.
- To provide technical support for application development team as a form of a help desk.
- To enforces and maintains database constraints to ensure integrity of the Database.
- To Administers all database objects, including tables, clusters, indexes, views, sequences, packages and procedures.
- To Assists with impact analysis of any changes made to the database objects.
- To troubleshoots the problems regarding the databases, applications and development tools.
- To manage sharing of resources amongst applications.

18.6 DBA Skills

- A good knowledge of the operating system(s)
- A good knowledge of physical database design
- Ability to perform both database and also operating system performance monitoring and the necessary adjustments.
- Be able to provide a strategic database direction for the organization.
- Excellent knowledge of database backup and recovery scenarios.
- Good skills in all database tools.
- A good knowledge of database security management.
- Sound knowledge of the applications at site.
- Experience and knowledge in migrating code, database changes, data and menus through the various stages of the development life cycle.
- A good knowledge of the way database enforces data integrity.
- A sound knowledge of both database and program code performance tuning.
- A DBA should possess a sound understanding of the business.
- A DBA should have sound communication skills with management, development teams, vendors, systems administrators and

19 INFORMATION SYSTEMS AUDIT POLICY

19.1 Introduction

Purpose of this audit policy is to provide the guidelines to security audit team to conduct a security audit on IT based infrastructure system at various departments of I2eConsulting Security Audit is done to protect entire system from the most common security threats which includes the following:

- Access to confidential data
- Unauthorized access of the department computers.
- Password disclosure compromise
- Virus infections.
- Denial of service attacks
- Open ports, which may be accessed from outsiders (Unrestricted modems unnecessarily open ports)

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Monitor all security measures to ensure conformance with I2eConsulting security policies
- Investigate security incidents recorded in security log book

19.2 Audit Policy

It is the responsibility of all Departments of I2eConsulting to place an appropriate system of internal audit, which provides an independent assessment of security policies. To execute these policies, internal audit should also be done and reports/documents based on these audit should be generated.

The system administrator or the nodal officer will be responsible for internal Audit within the department and operations of their sub dept.

When requested and for the purpose of performing an audit, any access needed will be provided to members of External Audit team. This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on respective Dept. equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to reports / documents created during internal audit.
- Access to interactively monitor and log traffic on networks.

19.3 **Questionnaire for Audit**

General

- Is departmental staff aware of I2eConsulting Security policies?
- Does the department have its own written security policies, standards and processes?
- Are these policies, standards and processes available in an easily accessed location? Please establish media type (hardcopy, electronic)
- Does staff have written guidelines for protecting their workstations and storage media files?
- Does the department have a system administrator?
- Are there clearly defined system security procedures for the Administrator?
- Is staff instructed on basic workstation security?
- Do personnel in your department have sufficient authority to accomplish IT security related duties and policies?
- Are there available and competent personnel to back up IT security related duties in the event the regular System Administrator is unavailable?
- Does the department have a process to address incidents or compromises?

On Hardware

- Is there redundant hardware to allow work to continue in the event of a single hardware failure?
- When were they last tested?
- Does the UPS notify someone when it goes into operation? When it was last tested?
- Is there a plan to have departmental hardware replaced at regular intervals?
- Does the department have system maintenance standards and procedures?
- Does the System Administrator/Nodal officer ensure that all sensitive data is removed from equipment before being sent out for repair or replacement?
- Is diagnostic hardware and/or software maintained onsite?

On Software

- Do you have original disks to reinstall the software if the hard drive fails? Is all

software supported? If your software is old or unsupported, what are your plans to replace it?
- Is locally developed software supported by an easy to reach developer?
- Do you have provisions to continue operation if central services software is not available?

On Environmental Failures

- Is your equipment situated in locations that are safe and free from potential danger (i.e., leaky roofs, sufficient power sources, etc.)?
- Do Uninterruptible Power Supplies (UPS) protect servers and workstations?
- Is the heating, cooling and ventilation keep your systems at the appropriate temperature and humidity?

On Accounts and Passwords

- Is there a departmental policy for selecting strong passwords?
- Is the department using software that enforces strong passwords?
- Are passwords changed? If so, how often?
- Is the department planning to use other forms of authentication other than passwords in the future?
- Does the department have an account removal process?
- Does the department have a method for identifying unauthorized users?
- Have staffs received computer security awareness training?
- Is there a document establishing the identity of those having root access to departmental information?
- Is the identity of those having remote access to departmental information known?
- Are there written procedures for forgotten passwords?
- Are there written procedures for closing accounts when an employee terminates employment?

Physical Security

- Has a physical security audit been done?
- Does the department have physical security standards and procedures?
- Are there procedures for locking computer rooms?
- Does the department have an alarm system?
- Are accesses secure when vacant?
- Are workstations and laptops locked down to deter theft?
- Are all workstations cases locked to prevent access to internal components?
- Are unused laptop computers kept in locked storage areas?
- Is Gate Pass Maintained when hardware is taken Out or in from the office?
- Does the department have a standard and procedure for sanitizing and disposing of confidential and sensitive material on hard drives, tapes, floppy disks, CDs, etc.?

On Network and Configuration Security

- Does the department have a network map/diagram?
- Does the department have an inventory of devices attached to the network?
- Are the room jacks mapped to a switch port?
- Is there a policy as to how network services are accessed by users?

- Does your department have network documentation to assist problem resolution of a computer or network device?
- Does your department have physical and remote access to your network devices?
- Does your department have the ability to continue to function in the event of a wide area network failure?
- Does your department have a network diagram that includes IP addresses, room numbers and responsible parties?
- Are end users prevented from downloading and/or installing software? How?
- Are contents of system logs protected from unauthorized access, modification, and/or deletion?
- Is the CD-ROM Auto run feature disabled on all workstations?
- Are the trusted workstations secured if used for other purposes?
- Are trusted workstations SSL or VPN enabled?
- Are trusted workstations required to have complex passwords?
- Are chat clients (ICQ, Yahoo Messenger, IM, etc.) managed? How are they managed?
- What security precautions are taken for dial-in modems?
- Are ActiveX, JavaScript, and Java disabled in web browsers and email programs for all workstations?

- Is the Administrator account, and any equivalent accounts, on all workstations limited to the office technical support person? Is it password protected?
- Is file sharing permitted and secured on any workstation in the department? If so, how is it secured?

On to Web Servers and Email

- Is the web server set to only accept traffic on port 80?
- Is the web server set to reject attempts to remotely administer it?
- Is the web server set to authenticate certain user traffic?
- Have the sample files, scripts, help and development files been removed? On FTP

- Are all FTP servers set to authenticate users?
- Is this traffic encrypted/secured?
- Are all FTP directories set to either Read or Write but not to both? On Email

- Is the E-mail server set to scan mail and attachments for viruses?
- Is the e-mail server set to reject attachments?
- Is web access to e-mail secured?
- Are client connections from outside the subnet secured/encrypted? On Disaster Planning

- Is there a written contingency plan to perform critical processing in the event that on-site workstations are unavailable?
- Do you have a plan to continue departmental working in the event that the I2eConsulting Central Systems are down for an extended

period?

- Do you have a partnership with vendors who can help in an emergency if your equipment is damaged due to disaster?
- Is the contingency plan periodically tested to verify it can be followed to resume critical processing?

On Backup and Recovery

- Are backup files sent off-site to a physically secure location?
- Are files kept on-site in a secure location?
- Are critical files regularly backed up?
- Do you store media off site?
- Is the environment of a selected off-site storage area (temperature, humidity, etc.) within the manufacturer's recommended range for the backup media?
- Are backup files periodically restored as a test to verify they are

usable? On Change Management

- Are records kept of systems changes?
- Is there a process for communication of systems changes?
- Does the department have a configuration/asset control plan for all hardware and software products?
- Does the department have a version control plan for software products?
- Are only trained authorized individuals allowed to install computer equipment and software?
- Are maintenance records kept to indicate what repairs and/or diagnostics were performed and by

whom? On Training

- Do you require new employees to read IT security documents?
- Does your staff know what's expected from them regarding security for your department?
- Would you consider a security workshop for staff provided by the Information Protection and Security Division?

Host based firewall

- Is critical data stored on a department server protected from compromise?
- Can you monitor if anyone is accessing critical data?
- Do you have enough technical staff to manage individual firewalls on all desktops? Network firewall?
- Are settings password protected?
- How often are logs reviewed?
- Is there central monitoring of settings and

logs?

Antivirus Software

- Are all workstations running the latest version of antivirus software, scanning engine and the virus signature file?
- Are users aware that email attachments should not be opened as a regular practice on PCs?
- Are employees aware of the dangers attachments can bring?

- What is the frequency for upgradation of virus definition?

20 ANNEXURE

20.1 Floppy disk:

A removable storage medium used with many computers. Also called a diskette, the medium itself is a single round disk of flexible, tape-like material that is housed in a square envelope or cartridge. Some floppy disks are recorded on only one side (single sided or SS); however, most are recorded on both sides (double sided or DS). It is used for storing computer data, readable by a computer with a floppy disk drive. These disks are known as "floppy" disks (or diskettes) because the disk is flexible and the read/write head is in physical contact with the surface of the disk in contrast to .Hard Disk. Which are rigid and rely on a small fixed gap between the disk surface and the heads.

20.2 Tape Drive:

A device used to store large amounts of data that are made up of cassette type reel to reel plastic tape. Tape Drive depends on Digital Data Storage (DDS) Technique, which is a format for storing and backing up computer data on tape that evolved from the Digital Audio Tape (DAT) technology. DAT was created for CD quality audio recording. Tapes conforming to the DDS format can be played by either DAT or DDS tape drives. However, DDS tape drives cannot play DAT tapes since they can't pick up the audio on the DAT tape.

DDS uses a 4-mm tape. A DDS tape drive uses helical scanning for recording, the same process used by a video recorder (VCR). There are two read heads and two write heads. The read heads verify the data that has been written (recorded). If errors are present, the write heads rewrite the data. When restoring a backed-up file, the restoring software reads the directory of files located at the beginning of the tape, winds the tape to the location of the file, verifies the file, and writes the file onto the hard drive. DDS cannot update a backed-up file in the same place it was originally recorded. In general, DDS requires special software for managing the storage and retrieval of data from DDS tape drives. There are four types of DDS drives:

- DDS-1: Stores up to 2 gigabytes of uncompressed data on a 120-minute cartridge.
- DDS-2: Stores up to 8 GB of data in compressed format on a 120-minute cartridge. DDS-2 is ideal for small network servers.
- DDS-3: Stores up to 24 GB of data on a 125-minute cartridge. The DDS-3 drive is ideal for medium-sized servers. DDS-3 uses PRML (Partial Response Maximum Likelihood). PRML eliminates electronic noise for a cleaner data recording.
- DDS-4: The newest DDS drive, DDS-4 stores up to 40 GB of data on a 125- minute cartridge.

  Small to mid-size businesses benefit from the DDS-4 drive.

A DDS cartridge needs to be retired after 2,000 passes or 100 full backups. DDS tape drive should be clean in every 24 hours with a cleaning cartridge and discard the cleaning cartridge after 30 cleanings. DDS tapes have an expected life of at least 10 years.

20.3 CD-ROM:

Stands for Compact disk-read only memory, which is not able to write data to disks without CD-Writer Capable of storing 650MB of data and normally used for storing operating systems, application programs, and multimedia programs. CD-ROM is of two types CD-R and CD-RW.

CD-R

- Disks that can be read and written through CD-writer.
- Disks can only be written to .once..
- Drives those are capable of reading and writing

data. CD-RW

- Disks that can be read and written.
- Disks are erasable.
- Disks can be written too many times.
- Drives those are capable of reading, writing and erasing

data. DVD- stands for digital videodisk.

- Uses similar technology as CD-ROM.
- Capable of storing up to 17GB of data.
- Data transfer rate comparable to hard disk drive.
- Compatible with CD-ROM disks.
- DVD-RAM- Ability to read/write data.

20.4 USB flash Drive

Plugs into the USB Port on laptop, PC, or Workstation. The USB flash Drive is available in 16,
32" 64, and 128 MB. This Drive takes advantage of USB Plug and Play capability Saves and backs-up Documents and any File presentations which provides an excellent solution for mobile and storing data as a reliable Data retention media.

20.5 Zip Drive

is a small, portable disk drive used primarily for backing up and archiving personal computer files. Zip drives and disks come in two sizes. The 100 megabytes size actually holds 100,431,872 bytes of data or the equivalent of 70 floppy diskettes. There is also a 250 megabyte drive and disk. Zip drive comes with a software utility that provides the facility of copy the entire contents of hard drive to one or more Zip disks. In addition to data backup, following are the suggestions for its additional uses:

- Archiving old e-mail or other files that are not in use any more but might be accessed someday.
- Storing unusually large files, such as graphic images that you need infrequently
- Exchanging large files with someone
- Putting your system on another computer, perhaps a portable computer

- Keeping certain files separate from files on your hard disk (for example, personal finance files)

The Zip drive can be purchased in either a Parallel or a Small Computer System Interface (**SCSI**) version. In the parallel version, a printer can be chained off the Zip drive so that both can be plugged into your computer's parallel port.

Document Control -

Organization	i2e Consulting Pvt. Ltd.
Title	IT Information & Security Policy
Author	Ghanshyam Panchal
Filename	IT Information & Security Policy v 1.25
Owner	Ghanshyam Panchal
Subject	Details and Information on Security Policies of IT
Review Date	14-Mar-2020
Reviewed	Ghanshyam Panchal

Document Approvals –

Approval	Name	Date
Approved	Vishal Rane	20-Apr-2020