

IT SYSTEMS – SECURITY POLICY

1. Policy Statement

- 1.1. The TEi board views IT services as valuable business tools. The organisation wishes to gain benefit from the use of IT services without subjecting itself to undue risks through security weaknesses or misuse.
- 1.2. IT services include all services which use information technology including but not limited to PCs, software, e-mail and the Internet.

2. Detailed Policy Elements

- 2.1. Detailed policy elements specific to particular IT services are included as appendices to this policy. These are:
 - Appendix A – Email
 - Appendix B – Internet Access
 - Appendix C – Security

3. Policy Elements

- 3.1. General Exclusions on Usage
 - a) No employee shall:
 - i) Use, or allow any other person to use, TEi procedures to access the systems of any other organisation or individual without their permission or in an unauthorised way.
 - ii) Disclose any information to unauthorised parties outside of TEi Ltd, which would allow those parties access to TEi Ltd's own systems or those of its partners, suppliers, customers or employees.
 - iii) Use, or allow any other person to use, TEi Ltd's systems to gain access to, store, modify or distribute material which could be considered to bring the name of TEi Ltd into disrepute or is illegal in nature.
 - iv) Use the TEi Ltd's IT resources for personal monetary gain, nor for commercial purposes that are not directly related to TEi's business.
 - b) No employee shall participate in any activities via IT services which could reasonably be considered to bring the name of TEi Ltd into disrepute.
 - c) No employee shall make or send calls or emails that are unsolicited or of an offensive nature, these will be considered as bringing the name of the TEi Ltd into disrepute. An unsolicited call or email is any that the recipient would not reasonably expect to receive from the originator.
 - d) No contract should be entered into using IT services, unless the Management board or nominee has given prior approval.
 - e) A high standard of conduct is expected of employees using IT services. Defamation or harassment of colleagues or others using IT services is prohibited.
 - f) If an employee receives a telephone call or message through any IT service which they find offensive, they may inform their manager. In such circumstances do not delete any such message from any storage system unless instructed to do so. The IT Department will, where necessary, carry out an investigation before referring the matter to the TEi Board, and will use absolute discretion.

- g) IT resources are not unlimited. Network bandwidth and storage capacity has finite limits, and all Users connected to the network have a responsibility to conserve these resources. As such, the User must not deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others. These acts include, but are not limited to unauthorised use of the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses.
- h) Employees are required to hand over all business related IT equipment, records and documents in their possession if they leave the employment of TEi Ltd.

3.2. Personal Use and Responsibility

- a) TEi's IT services are for business use. Occasional and reasonable personal use is permitted provided it is normally carried out in the employee's own time.
- b) Through its monitoring systems TEi Ltd's board has the ability to identify personal use, and reserves the right to raise invoices for the appropriate charges. TEi Ltd retains the right, following disciplinary proceedings, to raise invoices for charges where misuse of the policy has occurred.
- c) Where an employee, for their own use, using IT Services, purchases goods or services, then this is done at the employees own risk.

3.3. Systems Access

- a) Employees must keep all passwords and security codes secure.
- b) Employees will be held responsible for all activity using any IT system (including mobile phones, login accounts for computer services) they have been given access to. Employees should take precautions to stop unauthorised use when away from their desks (including the locking of screens).
- c) Individuals with access to TEi's IT systems and who are found to have:
 - i) Damaged the Executive's own computer systems, or those of another organisation
 - ii) Attempted to access a system or information within a system whether controlled by TEi Ltd or another organisation without the controlling organisations authority
 - iii) Attempted to exceed the facilities or privileges granted to them, whether through deliberate or negligent action may be subject to TEi Ltd's disciplinary procedures.

3.4. Representation of TEi Ltd

- a) No user shall purport to, or allow any other person to purport to, represent the TEi Ltd except in areas where they have the authority to do so.
- b) Any personal statements not directly connected with the business of the company must contain a clear statement to the effect that "This is an individual view and not necessarily an expression of the views or policy TEi Ltd.

3.5. Data Protection Act 1998

- a) All electronic content is subject to the Data Protection Act 1998. Under the terms of the Act, personal data includes any information about a living identifiable

individual, including their name, address, phone number, email address and any other information about the individual. If employees include such information they are deemed to be “processing” personal data and must abide by the law. Please refer to Data Protection Act guidelines for further information.

- b) Do not send other peoples personal details by email unless the recipient is verifiably the correct person and you have the correct permissions.
- c) In the event of TEi Ltd receiving a Subject Data Access Request, under the Data Protection Act, the Executive retains the right to search IT systems for the requested information. Wherever possible employees will be informed that this will occur prior to the search taking place, this however may not always be possible, in which case employees will be notified after the search.

3.6. Monitoring Of Systems

- a) The IT Department is responsible for the operation of any traffic, usage and connection monitoring systems which the Executive determines should be operated. Information from such systems may be passed to Management to enable decisions on investment to be made and an understanding of the usage patterns of TEi Ltd IT systems to be gained.
- b) TEi Ltd routinely runs monitoring reports on all users of all IT Services to assist with the management of IT resources.
- c) TEi Ltd has, and will maintain, the ability to monitor specific individual usage of IT Services including Internet and email services.
- d) TEi Ltd reserves the right to carry out audits of the use of any IT service at any time.
- e) In the event that an employee is absent from work and unable to give timely authorisation for access to be granted, TEi Ltd retains the right to check IT services for business related correspondence when there is a justifiable business reason.
- f) Permission for access to employee systems in these circumstances will be required from a Management Board Attendee, prior to the employee’s Line Manager or other nominee being able to access the relevant system. Access to the employee’s system will be removed as soon as reasonably possible following the individuals return to work or notification that such access is no longer required.
- g) Routine manual inspection of the content of electronic information will not take place. Manual inspection will only occur if there is good reason to believe that the employee’s usage:
 - i) contravenes criminal law,
 - ii) contravenes his/her employment contract,
 - iii) contravenes any policy of the Executive,
 - iv) contravenes discrimination law,
 - v) amounts to a civil wrong (such as defamation),
 - vi) means aspects of this policy are being broken,
 - vii) or is required to protect health and safety

Employees will be informed before any manual inspection takes place if appropriate or possible, unless the search is subject to paragraph h.

- h) Should the directors detect use of a system, or information obtained from any system, by its employees that could be deemed to appear to contravene United Kingdom or International law, the matter will be referred in the first instance to the management board and the company Secretary. The Management Board will decide whether the matter should be referred to the Police or other official body without notifying the employees involved.
- i) It is likely that any telephone call, email message or access of Internet sites is being logged or recorded by others as well as the management board. The policies of other organisations will vary from TEi Ltd. As a result there is no guarantee of safety, security or anonymity when using unsecured IT services.

3.7. Software

- a) TEi Ltd is committed to using software for which it is properly licensed and will not accept the use of unlicensed software or more copies of software than it has licences.
- b) All computer software must be purchased through the IT Department. No user may purchase software by any other means
- c) Software must not be installed on any equipment unless carried out either by the IT Department or with their express permission.
- d) There must be no transferring of software between computers without the express permission and involvement of the IT Department.
- e) It is forbidden for employees to load and operate software obtained from the Internet, via e-mail, magazine gifts or other sources including 'public domain', 'shareware', 'freeware' or 'evaluation' software without the prior permission of the Head of Information Technology or nominee. This will only be granted in the event of suitable testing having taken place and the management board having or being able to obtain an acceptable licence for the software.

3.8. Copyright

- a) Users may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licences that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a licence or download any material without first obtaining the express written permission of the management board or nominees as appropriate.

3.9. Delivery of information using some IT services (e.g. external email or faxes) cannot be guaranteed, neither can the authenticity of the recipient, therefore if the content of a message is confidential or time critical then the sender should ensure that the message has been delivered and the correct person has received it.

3.10. The IT manager & Directors will decide if there has been any infringement of the contents of any part of this policy, including the appendices of this policy, which may subsequently be subject to the company disciplinary procedures.

3.11. This policy should be read in conjunction with the company IMS procedures.

APPENDIX A – EMAIL

1. Disclaimer

- 1.1. The ability for staff to send emails to individuals and other organisations using the Internet is a key business requirement. The provision of this service leads to the risk of unsolicited emails being received by an employee (commonly called spam). The Management Board uses appropriate tools to stop as many of these emails as possible from reaching employees email accounts, some of which may be offensive to some employees. These tools will be maintained to ensure the protection is as effective as possible. It is not however possible to stop all unsolicited emails from reaching employees email accounts.

2. General Exclusions on Usage

- 2.1. Email should not be used to download or import software onto TEi Ltd systems without the prior permission from the IT Manager or nominee. This includes software and shareware available on the Internet that may be received by email even if it is apparently free.
- 2.2. Connection to the Internet for the purposes of email will be through appropriate security systems, the configuration and performance of which will be the responsibility of the IT Department. The connection, within Executive premises, of PCs to the Internet except via appropriate security systems is forbidden.

3. Personal Use and Responsibility

- 3.1. TEi Ltd's IT services are for business use. Occasional and reasonable personal use is permitted provided it is normally carried out in the employee's own time.

4. Representation of the Executive

- 4.1. Full company contact information will be attached to all external emails stating the business address and other required details under the Business Names Act 1990.
- 4.2. All personal statements not directly connected with the business of TEi Ltd must contain a clear statement to the effect that:
This is an individual view and not necessarily an expression of the views or policy of TEi Ltd.

Employees must include this text themselves, as it will not be included automatically.

5. Monitoring of Emails

- 3.1 All emails received by TEi Ltd from external sources will be passed through anti-virus software before it reaches employees account. As part of this process certain generic categories of email attachments (lists of which will be issued from time to time) will be automatically intercepted due to the risk of virus or other malicious software being imported in TEi Ltd's systems. If an employee is uncertain about the source or content of an email attachment then they should contact the IT department before opening the attachment.

APPENDIX B – INTERNET

1. Disclaimer

- 1.1. Users are cautioned that many of the pages on the Internet include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk and TEi Ltd is not responsible for material viewed or downloaded by users from the Internet.

2. General Exclusions on Usage

- 2.1. Employees deemed to be accessing or attempting to access inappropriate sites deliberately or for a time exceeding that associated with an innocuous search may lead to disciplinary action. Inappropriate sites are those that other employees may find intimidating, upsetting, embarrassing, humiliating or offensive.
- 2.2. The Internet should not be used to download or import software onto the TEi Ltd systems without the prior permission from the IT manager or nominee. This includes software and shareware available on the Internet even if it is apparently free, including but not limited to screen savers, games and other applications.

3. Personal Use and Responsibility

- 3.1 TEI Ltd's IT services are for business use. Occasional and reasonable personal use is permitted provided it is normally carried out in the employee's own time. Reasonable personal use of email and the internet should be kept to a minimum.

4 Internet Access

- 4.1 Connection to the Internet for any purpose will be through appropriate security systems, the configuration and performance of which will be the responsibility of the IT Department. The connection, within TEi Ltd's premises, of PCs to the Internet not via appropriate security systems is forbidden.
- 4.2 TEI Ltd has the right to, and will utilise software that makes it possible to identify and block access to Internet sites, other services that use a disproportionate amount of the TEi Ltd Internet resources or where these sites are not directly related to its business.
- 4.3 Access to Internet services of any sort must be requested from the IT manager nominee. Requests should be through the IT manager for new staff or otherwise by email or memo from departmental heads responsible for the work area in question, giving brief reasoning behind the request.
- 4.4 Where such access can be granted within existing systems and there are no major technical barriers, such access will be granted subject to the employees agreeing to abide by this policy.

APPENDIX C – SECURITY

1. Physical Access

- 1.1. All confidential and licensed material will be held in secure cabinets and only available to authorised people. These authorised people will be required to sign a log book when items are removed and returned.

2. Personal and Laptop Computer Security

- 2.1. It is the responsibility of each user to take all reasonable precautions to safeguard the security of the computer and the information contained on it. This includes protecting it from physical hazards, including spilling liquids; not allowing unauthorised users access to the machine and only using approved software.
- 2.2. Documents stored on laptop hard disks or the C: drive of a PC are not backed-up and cannot be recovered if deleted. In the event of theft the documents are open for anyone to view.
- 2.3. Storage of documents on a laptop C: drive or re-movable hard drives of PCs should be for as short a time as possible to minimise the risk of data loss.
- 2.4. Users are reminded of their extra responsibilities when they are in possession of a laptop computer to use either on or away from TEi Ltd premises. Laptop computers, PDA's or similar devices must be secured when left unattended for any length of time and should not be left out unsecured on desks overnight.

3. Network Security

- 3.1. The transfer of confidential information over unprotected communication links will be restricted, whether within TEi Ltd's private network or via the public network. There will be sufficient safeguards in place to prevent unauthorised persons from accessing TEi's IT systems. Where there is a need to connect with the public or other network outside of the control of TEi this will be via an appropriately configured "firewall".
- 3.2. A minimum level of security will be maintained across all computer systems, the required level of security and controls will be determined by the highest level of confidentiality of the information handled. Where data is replicated across different elements of the network, sufficient safeguards will be put in place to ensure that the information is kept in step.

4. Connection of Non- TEi Ltd IT equipment to the TEi Ltd network

- 4.1. The normal method of exchanging information between TEi Ltd and its suppliers or other bodies will be through Internet email. Direct connections to TEi Ltd mail systems will not be permitted.
- 4.2. Where automated exchanges of information are required (electronic data interchange; EDI), suitable EDI facilities must be built into the packages, products or database applications used. Responsibility for ensuring that such features are specified rests with the managers controlling the acquisition process for the software involved.
- 4.3. Under normal circumstances, direct access to TEi Ltd's IT systems by suppliers or other associated bodies will not be permitted. It is recognised, however, that where there are close relationships with clients involved with major parts of the TEi Ltd's business, such direct access may be required. In such cases the business case

must be agreed between the requesting manager and the IT manager. This must explicitly cover the provision of adequate security.

- 4.4. Connection of individuals own PC's to the TEi Ltd networks by any method will only be allowed if prior agreement has been given by the IT manager.

5. Passwords

- 5.1. The username and password given to employees, agents and suppliers to allow access to IT resources are for the use of the individual for whom the account is created. Passwords must never be shared with anyone.
- 5.2. If there is a need to allow someone to access information you have on the computer systems then this can always be done by means other than password sharing. Contact the IT manager for assistance.

6. Internet Security

- 6.1. All information downloaded from the Internet will be automatically scanned for viruses, this will also include attachments which are received by external e-mail.

7. Mechanisms for reporting actual or suspected security incidents

- 7.1. All employees of TEi Ltd have a duty to report any actual, attempted or suspected breach of IT security as soon as practical.
- 7.2. Such reports should be passed to the IT Dept, and suitable action will be taken.