joining up journeys SPT

Strathclyde Partnership for Transport

IT & Information Security Policy

Policy

1. Statement of Policy

INTRODUCTION

1.1. SPT has experienced a considerable increase in the use of information technology (IT). Usage of IT services is set to continue growing in light of the Government's initiatives for Best Value and Electronic Service Delivery.

1.2. It is essential that all information processing systems within SPT are protected to an adequate level from disruption and loss of service, whether through accident or deliberate damage.

1.3. This document has been produced in line with the Standard for Information Security (ISO 27001:2005) which is acknowledged as the appropriate standard for a security policy.

1.4. The document outlines SPT's policy in relation to the use of electronic devices and information and especially in the areas of:-

- Fraud
- Theft
- Use of unlicensed software
- Private work
- Hacking
- Sabotage
- Misuse of personal data
- Use of the Internet and email
- Disposal of Equipment

PURPOSE OF THE SECURITY POLICY

1.5. The purpose of the policy is to provide a set of rules, measures and procedures that determine SPT's commitment to ensuring that its IT resources are protected from physical and remote threats.

1.6. The main objectives of the policy are:-

- To ensure that all SPT's assets, staff, data and equipment are adequately protected against any action that could adversely affect the IT services required to conduct SPT's business;
- To ensure that Staff and Partnership Members are aware and comply with all relevant legislation and SPT policies related to how they conduct their day-to-day duties in relation to IT.

2. Scope of Policy

The policy is relevant to all IT services, irrespective of the equipment in use, or location, and applies to:

- All Employees, Contractors and agents;
- Employees and agents of other organisations who directly or indirectly support or use SPT's ICT Services;
- All use of IT services within SPT.

3. Legislation

3.1 SPT has to comply with all UK legislation affecting IT. All organisations, employees, Partnership Members and agents must comply with the following Acts and they may be held personally responsible for any breach of current legislation as listed below.

3.2 The following are brief descriptions on 'key legislation' affecting IT users. Do not assume that this covers all your legal responsibilities. If you are in any doubt about your legal responsibilities ask the Legal Department for assistance.

3.2.1 Data Protection Act 1998

- Computers are in use throughout society – collating, storing, processing and distributing information. Much of the information is about people - 'personal data'. This is subject to the Data Protection Acts.

- SPT is only allowed to record and use personal data if, under the Acts, there is a legitimate purpose for doing so and if details of the information, its use and source have been registered with the Data Commissioner. There are strict rules about how the information is used and to whom it is disclosed.

- The Act gives rights to individuals about whom information is recorded on computer and in certain manual files. They may request copies of the information about themselves challenge it if appropriate and claim compensation in certain circumstances.

- If there is any doubt about whether the information can be collected, used or disclosed please address queries to SPT's Information Officer.

- A separate policy document covering the responsibilities under the Act is available via SPT's Intranet site or from the Information Officer direct.

- http://www.dataprotection.gov.uk/

3.2.2 Copyright, Designs and Patents Act 1988

- Under this Act, any duplication of licensed software or associated documentation (e.g. manuals) without copyright owner's permission is an infringement under copyright law. All proprietary software manuals are usually supplied under licence agreement, which limits the use of the products to specified machines and will limit copying to the creation of backup copies only. However in some instances, site licenses, permitting the use of software on all machines within a specified site are obtainable.

- To combat the problems of illegal copying, software suppliers have formed their own organisation to police the use of software throughout the UK. The 'Federation Against Software Theft' (FAST) is able to conduct 'spot' checks on organisations, including local authorities, under a court order and without prior warning.

- According to the Act, individuals found to be involved in the illegal reproduction of software may be subject to unlimited civil damages and to criminal penalties including fines and imprisonment.

- http://www.fast.org.uk/

- http://www.hmso.gov.uk/acts/acts1988/

3.2.3 Computer Misuse Act, 1990

- The Computer Misuse Act, 1990 was introduced to deal with three specific offences that were not adequately covered under existing laws:

  - Unauthorised access or attempt to access computer material (such as logging into the SPT network using other employees' credentials). Under this offence it is not necessary to prove the users intent to cause harm;

  - Unauthorised access with intent. For example, hacking is carried out with the intention of committing a more serious crime such as fraud. Under this offence, if a plan has been hatched which involves the unathourised use of a computer, the unauthorised use will be sufficient to prove an attempt to commit the crime;

  - Unauthorised modification. This part of the act makes it an offence to intentionally cause unauthorised modification such as the introduction of viruses.

- The intention of the act is to enable an organisation to take legal action to protect their data and equipment from unauthorised access and damage.

- http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

3.2.4 Health and Safety at Work etc. Act (1974)

- SPT shall ensure, through the appointed Health and Safety Officer that all IT equipment is located and used in such a way to not impede health of users or others.

- http://www.hse.gov.uk/legislation/hswa.htm

3.2.5 Human Rights Act 1998 (operative October 2000)

- Under this Act, everyone has a right to respect for their private life, their home and correspondence, which is commensurate with the need to protect SPT from fraud, introduction of viruses or breach of other overriding considerations. To this end, SPT reserves the right to monitor usage of PC's and telephones.

- Individuals using the Internet, e-mail or telephone should respect the confidence of SPT and colleague's information in disclosing it to other people. E-mail, in particular, should not be circulated in a tone, which may give rise to a claim of inhuman or degrading treatments.

- http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Procedures

4. Rules

4.1 MANAGEMENT OF THE POLICY

a. IT and Information security is the responsibility of all members of SPT staff. The IT Steering Group (ITSG) is responsible for monitoring and reviewing the policy on behalf of the Partnership.

b. The policy has been reviewed by the Chief Internal Auditor in terms of the policy's scope, content and effectiveness. The Chief Internal Auditor will periodically review this policy as part of the strategic plan.

c. The ITSG will nominate an Information Security Officer whose responsibilities will include implementing, monitoring, documenting and communicating information security in compliance with the security policy and legislation.

d. Managers, administrators and individuals are responsible for ensuring that all staff are aware of their responsibilities under the policy and have access to the contents of this document and its associated User Guide ('SPT ICT User Guide').

e. All providers of IT-based services must ensure the security, integrity and availability of data within the service provided.

f. The IT & Information Security Policy is intended to be a living document, which will be updated, as and when necessary. Sections and appendices can be added to reflect new or amended procedures and guidelines when determined.

4.2 VIOLATIONS

4.2.1 Violations of this policy may include, but are not limited to, any act that:

- Exposes SPT to actual or potential monetary loss through the compromise of IT security;
- Involves the disclosure of confidential information or the unauthorised use of corporate data;
- Involves the use of data, which causes, for example, the law to be broken.

4.2.2 Any individual who suspects that this policy is being violated by another individual must report the violation immediately to his or her Manager, who must report the matter to the Director of HR&OD or the Senior Technology Solutions Advisor.

4.2.3 A log of all security incidents will be kept by the Technology Solutions Department. The log is the responsibility of the Service Support Team Leader. The log records any reported incidents and action taken.

4.2.4 Internet use and access to web sites can be monitored. **Any breach of IT Policy will lead to disciplinary action against the individual concerned.**

5. Responsibilities

All Employees, Contractors and agents are responsible for complying with this policy and maintaining the integrity of SPT IT infrastructure and data.

6. Definitions

N/A

7. Arrangements

7.1 ASSETS CLASSIFICATION AND CONTROL

7.1.1 The Technology Solutions department positively identifies and keeps documentary evidence of all computer equipment. It is the responsibility of the Service Support Team Leader to ensure that these records are accurate and continuously maintained.

7.1.2 Each inventory item must clearly identify each asset by an identity tag detailing its unique asset number.

7.1.3 The inventory is maintained using a database, including information relating to location, user, asset tag number, and serial number.

7.1.4 On receipt of new equipment it must be labelled and recorded on the inventory. No IT equipment should be purchased without prior consultation with the Senior Technology Solutions Advisor.

7.1.5 No equipment should be installed on SPT's network without prior consent of the Senior Technology Solutions Advisor or Service Support Team Leader who must first record the equipment within the inventory.

7.1.6 All disposals of equipment should be recorded against its original entry. SPT actively pursues a 'green policy' on recycling IT equipment.

7.1.7 A regular percentage audit of equipment should be carried out by the Service Support Team Leader and the Chief Internal Auditor.

7.1.8 No equipment should be relocated without prior consultation with the Senior Technology Solutions Advisor or the Service Support Team Leader.

7.2 PERSONNEL SECURITY

Security in Job Definition and Resourcing

7.2.1 The Director of HR & OD should ensure that there is adequate definition of responsibilities in relevant Job Descriptions for security responsibilities.

7.2.2 All Staff commencing employment with SPT agree to comply with this policy and its associated 'E-mail and Internet Policy' and 'SPT ICT User Guide'.

7.2.3 Personnel procedures ensure that all Staff are made aware of these policies during their 'induction process'.

7.2.4 Copies of all the policy and guidance notes are available from via SPT's Intranet site. Staff are to sign as having read and understood the IT Policy documents.

7.3 PHYSICAL SECURITY AND ENVIRONMENTAL SECURITY

Physical Access Controls

7.3.1 All Staff are issued with identification badges and these should be carried at all times during working hours. The transfer of badges, keys and other security devices is prohibited. Officers leaving employment with SPT must return all badges, keys and portable computer equipment they have responsibility for.

7.3.2 Supervising Officers have a responsibility for ensuring that Staff leaving SPT's employment account for their identity badges, keys and portable computer equipment.

7.3.3 An identification badge grants access to staff-only areas of SPT. All Visitors to SPT premises are issued with visitor passes.

7.3.4 No member of Staff should take responsibility for a guest or contractor within staff-only areas without ensuring the individual has been issued with a visitor pass. Guests should be supervised throughout the duration of their visit.

7.3.5 SPT has security-coded access to restricted areas. Security codes to these areas are changed at periodic intervals.

7.3.6 Access to the Server Suite is clearly defined as a security perimeter. Access is controlled by Security coded doors. Only staff who have legitimate business and whose jobs require it should be allowed to enter areas where computer systems are located.

7.3.7 No staff or Guests are left unsupervised whilst in this secure area.

7.3.8 Staff who have suspicion about the identity of an individual within a staff-only area are instructed to politely ask them to determine the purpose of their visit. Employees who are uncomfortable with this responsibility are instructed to report the incident to a Senior SPT Officer immediately.

7.3.9 Loss of identity badges or keys must be reported to the Head of Security as soon as the loss is discovered.

Security of Equipment

7.3.10 Where possible Computer equipment is sited away from public areas. Where this is not possible the equipment is always supervised.

7.3.11 Computer screens and printed output should not be in view of unauthorised persons.

7.3.12 All computer screens that are in public areas should be controlled by time delayed screensavers which require a password to access information.

7.3.13 Staff should take responsibility for the physical security of their Computer Equipment within their working environment. Windows and doors should be kept shut whilst unattended.

Power Supplies

7.3.14 Critical equipment is protected from potential power loss by uninterruptible power supplies (UPS).

7.3.15 All UPS's are periodically tested and upgraded where necessary.

Cable Security

7.3.16 All networking devices (i.e. routers) are securely located within SPT premises.

7.3.17 Power and Telephony lines into SPT premises are underground where possible.

7.3.18 Data transmissions between remote locations are either carried over proprietary fibre, encrypted or dedicated leased lines.

Equipment Maintenance

7.3.19 All equipment is maintained to ensure availability. Critical systems are supported by annual maintenance agreements, which provide for Technical Support and call out.

7.3.20 IT equipment is maintained by Technology Solutions. Repairs and servicing should only be carried out by authorised Staff and Contractors.

7.3.21 A record of all faults is maintained by the Service Support Team Leader. Staff who wish to report faults of their equipment are able to do so by reporting the incident to the Technology Solutions Service Desk on Ext 3731.

7.3.22 Staff are issued with a 'call reference number' to provide an audit trail for their call.

Security of Equipment off-premises

7.3.23 Before equipment (with the exception of laptop computers, mobile telephones and PDAs) can be removed from SPT premises a member of Technology Solutions must book it out.

7.3.24 Equipment used outside of SPT premises is only to be used for work purposes.

7.3.25 Portable computers are very vulnerable to theft; loss and unauthorised access when travelling. Personnel who have portable equipment should acquaint themselves with the instructions included in the 'SPT ICT User Guide'.

7.3.26 ICT equipment or media must not be left in an unattended vehicle. All portable computer equipment is insured with SPT's Insurance Officer, except when left unattended in a vehicle.

Equipment Disposal

7.3.27 All items of equipment containing storage media are only disposed of after reliable precautions have been taken to destroy the media.

7.3.28 A record is maintained of all equipment that has been recycled or disposed of.

7.4 COMPUTER MANAGEMENT

Operational procedures

7.4.1 All regular operational procedures are fully documented.

7.4.2 Regular back-ups and documented procedures are kept of all fundamental systems, including:-

- General Operations of Technology Solutions and Recovery procedures.
- Shared network files.
- E-mail files.

Incident Management Procedures

7.4.3 All system and hardware failures are logged and recorded on the Service Desk software. The Service Delivery Team Leader is responsible for investigating, resolving the failure, and implementation of remedies to prevent reoccurrence.

Segregation of Duties

7.4.5 Segregation of duties are in place wherever practicable. The objective is to minimise the risk of negligent or deliberate misuse of computer systems.

Capacity Planning

7.4.4 The Network capacity is monitored to ensure that there are adequate system resources. These include processors, main storage, file storage, printers and other output devices.

Protection from Malicious Software

7.4.5 SPT uses antivirus software as a means of protecting itself from malicious attack.

7.4.6 All Servers and workstations are installed with up-to-date antivirus software. User files are scanned for viruses each time a user logs onto the network or attempts to access files from disk.

7.4.7 Technology Solutions staff periodically check to ensure that all workstations and Servers are updated with the most up-to-date version of antivirus software available.

7.4.8 Staff are instructed to report all Virus incidents, including 'hoaxes', immediately to the SPT IT Service Desk.

7.4.9 No staff should load or install software on any SPT computer without the prior consent of the Senior Technology Solutions Advisor.

7.4.10 No media should be loaded onto an SPT workstation without first being swept for viruses.

7.4.11 All staff are made aware of good practice for virus control including e-mail and Internet protocol (E-mail and Internet Policy).

Housekeeping

7.4.12 Technology Solutions staff regularly review data stored on the network to ensure that it continues to conform to operational requirements. Surplus data is archived or removed after consultation with the User.

Data Backup/Media Storage

7.4.13 Back-up copies are taken of all essential data, software and system files daily. The backup procedures ensure that all critical systems can be recovered in the event of a disaster.

7.4.14 Back-ups are checked daily to ensure that they have completed and records of all Back-ups are kept securely. This is the responsibility of the Service Support Team Leader.

7.4.15 All Back-ups are clearly labelled and are removed off-site weekly. Tapes are stored in fireproof safes. Documented procedures provide for the rotation of backups.

7.4.16 Backups consist of:-

- 4 weekly backup sets.
- 12 monthly backup sets.
- Year-end.

7.4.17 Backup procedures are tested regularly. Records are maintained of all successful restores.

Operational Logs

7.4.18 Operational logs are maintained of all work carried out. The log records details of the job and the time that processing commenced.

Fault Logging - Service Desk

7.4.19 The Service Desk exists for reporting faults to Technology Solutions. All Staff are aware of the Service Desk and are encouraged to report incidents to this single point of contact.

7.5.20 The Service Support Team Leader is responsible for responding to faults reported in accordance with the Services performance targets.

7.5.21 The Service Desk is also used to report 'network' and 'systems' faults and 'development' requests.

7.6 NETWORK MANAGEMENT

Network Security Controls

7.6.1 The Technology Solutions department are responsible for the security of data on the network and to protect connected services from unauthorised access.

7.6.2 The Senior Technical Solutions Advisor has responsibility for security access to the network.

Enforced Path

7.6.3 Users are set up with default network contexts. This prevents undesirable 'straying of users'.

Network Access

7.6.4 Network access is controlled by Technology Solutions staff.

7.6.5 Users and their access to resources are created, modified and deleted as appropriate when requested or notified by an authorising Officer. No access or amendment is made unless appropriate authorisation is received from the Data Owner.

7.6.6 Access by third parties (Software maintenance) to the Network is only allowed in the following circumstances:-

- The Systems Owner has confirmed in advance with the Senior Technology Solutions Advisor or Service Support Team Leader that maintenance is due to take place.
- The identity of the User has been notified to the Senior Technology Solutions Advisor or Service Support Team Leader.

7.6.7 Network modems are only activated on request. TS are responsible for logging third parties onto network resources. TS record access time and details and monitor usage until maintenance is complete, at which point the modems are switched off and Servers locked. Systems owners are responsible for checking that system maintenance is carried out is accordance with action agreed upon.

Media Data Handling Procedures (See also Data Back-up procedures)

7.6.8 No data is removed from Technology Solutions unless it is signed for or collected by an authorised employee.

7.6.9 All data is packaged accordingly to protect it during transit.

Security of System Documentation

7.6.10 All systems should be adequately documented. Documentation is kept current and matches the state of the system at all times.

7.6.11 Systems documentation is physically secured at all times with access restricted to authorised personnel. An additional copy should be kept (hardcopy or softcopy), which will remain secure in the event of the original copy being destroyed.

Media Disposal

7.6.12 All hardcopy media containing sensitive data is disposed of in accordance with SPT's corporate policy for disposal of sensitive data.

7.6.13 All magnetic data is destroyed if the equipment is to be disposed of. Where the equipment is to be recycled the magnetic data is reformatted or checked with specific software to clear the data. Where a third party Contractor is used to 'clear data' a legal disclaimer is required.

Security of Electronic Mail

7.6.14 ISO 27001 recommends a specific policy for e-mail. The protocols for sending and receiving e-mail are addressed in the SPT E-mail and Internet policy.

7.7 SYSTEM ACCESS CONTROL

Business requirement for system access

7.7.1 Systems and Data Owners should have clearly defined access policies, which determine the access rights for users and groups to their Data and Systems. The policy should take account of:-

- The security requirements for specific applications and systems.
- The policy for disseminating information.
- The need for access to carry out the duties as specified in their job description.

7.7.2 All Systems and Data Owners should consider the access they want to allow Users. Technology Solutions staff will give Users file permissions only on receipt of a formal documented request (See User Access Management) from the Systems and Data owner.

User Access Management

7.7.3 There is a formal user registration and deregistration procedure for access to networked services.

7.7.4 No User is allowed access to the network without a formal 'network access request' being submitted to the Senior Technology Solutions Advisor or Service Support Team Leader. The request, authorised by an appropriate Data Owner or Manager, should detail the User and the access rights they wish the User to have. There should be an adequate period of notification to Technology Solutions for new employees (3 days minimum).

7.7.5 No alteration to User rights is granted without formal written request from an Authorised Officer.

7.7.8 System access rights are withdrawn by Technology Solutions staff as soon as an individual leaves SPT's employment or changes jobs. Details of the accuracy of this information reside with the Director of HR & OD who will formally notify Technology Solutions. Department Heads and Managers are responsible for notifying TS when agency and contract staff start and finish.

7.7.9 A network account is maintained by Technology Solutions department, of each User. The account details the Users access rights and privileges.

User Password Management

7.7.10 No individual should be given access to a live system unless properly trained. All new Users should be provided with adequate training in the systems they will require access to. System Owners are responsible for ensuring that users have the adequate training before requesting User access to the 'live' system.

7.7.11 Users should keep their passwords secret and never disclose them to colleagues. It is a breach of this policy for Users to share passwords or sign-in other Users. Doing so can lead to disciplinary action.

7.7.12 All Users should change their passwords periodically. The IT system is designed to include password ageing by default when accounts are set up.

7.7.13 Where systems permit, Technology Solutions staff set password length to a minimum of 8 digits for all new accounts.

7.7.14 All passwords are conveyed verbally to new Users by Technology Solutions. Users are immediately prompted to change their password.

7.7.15 Passwords are not displayed when entering them.

7.7.16 Users who forget their passwords are instructed to contact the Technology Solutions Service Desk.

7.7.17 Technology Solutions verify the validity of the request before issuing a new password. The identity of the individual is always checked before issuing a revised password.

7.7.18 Technology Solutions maintain a record of previous User passwords. This prevents Users reusing a previous password within a 2 year period. High security and system administration passwords are only issued to Technology Solutions staff. These passwords are changed regularly.

User Responsibilities

7.7.19 Good password management guidance advocates the following:-

- Keep passwords confidential;
- Avoid keeping a paper record of passwords;
- Change passwords wherever there is any potential compromise in security;
- Select passwords with a minimum of eight digits;
- Avoid basing passwords on potentially guessable formats;
- Change passwords regularly

7.7.20 Users are instructed not to leave equipment logged on and unattended. Users should ensure that they are logged off systems and sessions.

Login Procedure

7.7.21 Users accessing the network must comply with the Security Policy. Prior to logging-on, Users may be prompted with a display notice warning users that 'the computer must only be used by authorised personnel'.

7.7.22 User accounts are disabled after three failed attempts. Users must notify the Technology Solutions Service Desk to regain access. A User will be asked to identify themselves before their account is reactivated.

7.7.23 All Users are prompted for a Username and Password. Users may only attempt to access the system using their own User credentials.

Application Access Control

7.7.24 System Owners define access and use of application systems.

7.7.25 Systems Owners control access to applications and are responsible for ensuring that they support the objective of this security policy.

7.7.26 System Owners should strictly control access to System Utilities within applications. Only authorised users should have access to these utilities. Managers are responsible for ensuring that there is adequate 'internal checks' carried out on the procedures exercised by these users

7.7.27 All application systems should provide adequate audit trails of transactions.

7.8 SYSTEMS DEVELOPMENT AND MAINTENANCE

New Projects

7.8.1 No formal feasibility studies should be carried out without initial consultation with the Senior Technology Solutions Advisor.

7.8.2 All projects with a significant IT content should be referred to the IT Steering Group for consideration.

7.8.3 New systems should follow a formal feasibility study of the options prior to selection.

7.8.4 All projects for new systems should consider the security requirements of the system to safeguard the confidentiality, integrity and availability of the information assets. This should be considered during the feasibility stage of the project. Consideration should include:-

- Control of access to information;
- Segregation of duties;
- Access to audit trail;
- Verification of critical data;
- Compliance with legislative requirements;
- Backup procedures;
- Recovery procedures;
- Ease of use
- Data Protection

Change Control Procedures

7.8.5 Any change to systems, files and data, should be undertaken in a controlled manner. All changes should be processed through the TS Change and Asset Manager, documented and tested prior to implementation.

7.8.6 There should be a separate 'test' environment set up for new applications. All new applications should be acceptance tested and signed off by the User before going 'live'.

7.9 BUSINESS CONTINUITY PLANNING

Risks and Planning

7.9.1 The Technology Solutions department has identified and maintains a record of business critical systems and processes.

7.9.2 The Senior Technology Solutions Advisor periodically reviews operational risks and the impact to SPT.

7.9.3 The Technology Solutions department holds a comprehensive IT Disaster Recovery Plan which includes critical IT business processes and recovery action.

7.9.4 Staff responsibilities will be determined and conveyed in the IT Disaster Recovery Plan.

7.9.5 All Staff responsible for Recovery procedures will be trained accordingly. Procedures are tested and reviewed regularly.

8. Training

8.1 Each new employee is made aware of his or her obligations for security during SPT's induction-training program. This includes Staff being told of the existence of the IT & Information Security Policy, the Email & Internet Policy and the 'SPT ICT User Guide'. Training on the proper use of ICT is available from TS on request.

8.2 Training requirements are reviewed on a regular basis to take account of the needs of the individual, and to ensure that staff are adequately trained in the use of technology.

8.3 Corporate IT training is the responsibility of the Human Resources & Organisational Development Directorate. Where training is required for a specific application this may be carried out in consultation with the Users Manager.

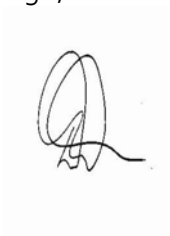
9. Review

The Senior Technical Solutions Advisor is responsible for reviewing this policy. This policy is to be reviewed under the following circumstances;

- Annually
- In the event of a major change that may affect the security of the IT infrastructure.

10. Approval (signature and date)

Sign;



Print;

Dean Drew

Date; **12/04/10**

Designation; **Senior Technology Solutions Advisor**