Information security policy

1.0 Introduction

The information that the council holds, and the Information Technology (IT) systems and networks that support it, are important business assets. Many potential threats to these assets exist, such as fraud, vandalism, virus infection, theft, abuse of copyright, misuse of software, and accidental damage.

Information security involves the protection of information for:

- Confidentiality: keeping sensitive information out of the wrong hands
- Integrity: making sure that information is accurate and complete
- Availability: ensuring information and services are available to users when required

We need information security:

- to make sure that the council can continue working without interruption
- to enable the council to share information whilst keeping that information accurate, up to date, and secure

2.0 Scope

This policy applies to all employees of South Lakeland District Council.

3.0 Principles

The council understands the importance of information security. The council is becoming increasingly dependent on IT and so the potential impact of any breach is also increasing. That is why we must safeguard our information systems and ensure that there is compliance with this policy. These procedures will protect the council, its employees and others we work with from consequences of loss, damage, misuse or prosecution."

This policy is based on the ten key controls for information security as defined in BS7799 (1995).

4.0 Key controls

4.1 Information security policy

It is essential that a written policy document is available to all employees. The overall policy of the council is set out in this document. All employees are required to read this document and the Internet and Email Acceptable Use Policy, they must also sign the Authorised User Agreement to indicate their acceptance of these policies before access to IT can be granted.

In addition to signing the policies, staff that have access to RESTRICTED data must go through the baseline security clearance checks before access to these services can be granted.

4.2 Allocation of information security responsibilities

Employees have specific responsibilities in relation to:

- The protection of individual assets
- Carrying out specific security procedures

The council's information technology and communications infrastructure is such that almost all the components are considered to be part of a single Network. It is the responsibility of the IT Services Manager to decide if and how any new assets are to be obtained and to approve how they are to be integrated into the network. No hardware should be acquired or attached to the network, and no software should be installed onto the network, without such approval.

4.2.1 Assets: Classification and control

Assets are things of value, the council owns many assets and this strategy aims to protect those that are related to the computer network in some way.

The Business Development Group is responsible for this policy and therefore the definition of what is to be considered as an asset and a security procedure under this policy. The Group assigns system administrators with responsibility for assets and procedures, where necessary with the guidance of the Management Team.

The Shared ICT Support Officer is responsible for maintaining a database of all assets. This describes the assets, which employee 'owns' them, and records any authorised uses and security procedures that relate to them.

These assets fall into three main types:

- Physical: such as computers, communications equipment, and media
- Software
- Information: databases, files, manuals and so on

Each asset is 'owned' by an employee who is responsible for it. This responsibility may include the execution of one or more procedures, such as backing up, related to the asset. Hardware and software are regularly audited, to ensure that no breaches of policy (such as the installation of illegal software) are taking place. Staff who use portable devices such as Tablet or Notebook PCs must be particularly vigilant, since these devices are more likely to be lost, damaged or stolen. Portable computers often have copies of files and emails on them, these devices must be password protected but this on its own doesn't provide 100% security. All portable devices must be encrypted using an approved method; if this is not possible due to device restrictions then the relevant service manager must carry out a risk assessment prior to the devices being deployed. The Risk assessment must cover the data stored on the devices and ensure that adequate protection is in place. Portables should not be left unsecured in public places. Where relevant, consideration should be given to the use of cable locks, which physically attach portables to desks.

Council equipment should not be taken abroad.

All equipment eventually becomes unusable or no longer fit for purpose. The council has procedures in place to deal with the disposal of IT equipment and they must be followed. It is vital to ensure that all data is destroyed to the appropriate level before any equipment is disposed of. The only exception to this is where an approved recycling organization is used to dispose of the equipment and they can provide a certificate of destruction before the equipment is handed over.

All IT equipment must be handed back to IT services so that it can be disposed of in the most appropriate way.

4.2.2 Personal security

As well as employees of the council, the term 'users' includes contractors, students volunteers and other members of the public granted access to the network.

4.2.3 System access control

System access control is achieved by means of unique user names and passwords. Security of these passwords is an essential component of this security policy. Each user is responsible for the security of their password. The Technical Manager is responsible for allocating new passwords to users. Password requirements are detailed in the password policy. Don't leave a PC that is logged in to the network unattended without locking the screen. Screensavers can do this for you automatically. Don't let anyone else know your password. Change your password regularly. Imagine if someone else used your machine while logged on as you, and they went to www.dodgy.com. It would look as if it was you who had visited that site.

4.2.4 Prevention of misuse of IT facilities

Although the council wishes to encourage the use of IT, and has therefore made facilities available for managed personal use, authorised users must not under any circumstances use IT facilities for the conduct of personal businesses or private commercial activity.

4.2.5 Computer and network management

The Infrastructure Manager is responsible for ensuring that clear and documented procedures exist for all operational computer systems considered important to the network. This will allow smooth running in the absence of staff normally responsible for those procedures.

4.2.6 Environmental controls

The Infrastructure Manager is responsible for ensuring the adequacy and smooth operation of a number of environmental controls, including:

- Uninterruptable Power Supplies (UPS) to all critical servers
- Air conditioning: including temperature and humidity monitoring both primary
- and backup

4.3 Information security education and training

Users must receive appropriate training in organisational policies and procedures, including security requirements and the correct use of IT facilities such as logon and password changing procedures. It is the responsibility of the line manager or supervisor (the budget holder for contractors) to ensure this training takes place. All new employees will be made aware of this policy, and asked to sign it, as part of their induction.

4.4 Reporting of security incidents

The Infrastructure Manager is the IT Security Officer. Security incidents should be reported as quickly as possible to the IT Security Officer or a senior officer. Employees should also note and report on any observed weaknesses in, or threats to, systems or services. Serious incidents should be logged by emailing the Help Desk, with the words ‘SERIOUS INCIDENT’ in the subject line. The Business Development Group will monitor any action required. With security threats, malicious incidents, and deliberate virus infection, HR will be brought in to commence disciplinary proceedings if appropriate.

Any significant security incidents will be reported to GovCert UK by the IT Security Officer, their website is http://www.govcertuk.gov.uk/ but submissions will initially be done via email to incidents@govcertuk.gov.uk using their report template.

4.5 Virus controls

Prevention is better (and less expensive) than cure. The Infrastructure Manager is responsible for developing and monitoring an anti-virus policy, to protect the council from computer virus infections and other similar harmful programs. The policy states that viruses will be automatically detected, whatever their source, without any action being required on the part of users.

A virus is a program which copies itself from one place to another, and which may cause serious damage to data and programs stored on a computer. A virus can exist on any computer storage medium; memory stick, CD, tape, hard drive, and so on. Viruses arrive from outside, which means they usually come into the building on memory sticks or cards, CDs or DVDs, or email attachments. Email itself is rarely harmful; it is primarily documents or programs attached to email that can contain viruses. If a virus is found on your machine, or on a USB stick or CD inserted into your machine, a warning message will appear. The virus will be quarantined automatically, but please contact IT Services immediately in case any additional action is required. If necessary, IT Services will remove the machine from the network and disinfect it.

Another source of viruses is the Internet. When you visit a web site, images and small programs (called applets) are automatically downloaded to your machine. Our anti-virus software will automatically detect any viruses before anything is downloaded. If you see a warning message, leave the web site, and contact IT Services. Viruses can be attached to macros that run inside Office applications. For this reason it is a good idea to disable macros, although this isn't mandatory. If you allow Office macros to run on your machine, you should be aware of the risks, and only run macros from a trusted source (such as those a colleague may have written).

If a computer virus is transmitted to another organisation, the council could be held liable if there has been negligence in allowing the virus to be transmitted. So always take care, don't open anything suspicious and if in any doubt contact IT Services. Viruses are a real threat, so you need to exercise caution. You should treat suspicious items like suspicious packages, don't open them. Either delete them or get advice.

4.6 Business continuity planning process

It is the responsibility of the Infrastructure Manager to prepare and test a disaster recovery plan. This document identifies the risks to information and services and the steps for reducing those risks, mitigating the potential impact of various types of disaster on business activities.

4.7 Control of proprietory software copying

Users must not copy licensed software and must not install or use unlicensed software. It's as simple as that. Material such as fonts, drivers, shareware or freeware must not be used without proper authorisation, even these types of software and

resources are regarded as assets and as part of the network. Software is protected by copyright in much the same way as books and music. The author owns the copyright, and no-one else is allowed to make copies, software comes with a license, which allows you to use the software, but does not grant you ownership.

Audit software automatically scans PCs for installed software on a regular basis, and the results are compared against the database of software licenses. Breaking copyright or licensing regulations is illegal. An organisation called FAST (Federation Against Software Theft) exists to seek out and prosecute individuals and organisations that do not comply. Theft is an act of gross misconduct. In addition, you need to be aware that much of the material on the web is protected by copyright. Just because an image or a document exists on the web, does not mean that you are free to copy, modify and distribute that image or document. So don't copy or download material, or publish it on the council website, unless there is express or implied permission to do so. The council retains copyright and intellectual property rights over material produced in the usual or normal course of an authorised user's employment, engagement or association.

4.8 Safeguarding of organisational records

Important records of the organisation should be protected from loss, destruction and falsification. The Business Development Manager will maintain an inventory of key sources of information as part of the asset registers. This register also classifies material, and acts as a link to data protection and freedom of information. It is the responsibility of the Infrastructure Manager to prepare a Backup Strategy to ensure that important files and information can be copied and protected from damage or loss. Further detail can be found in the Backup Strategy, which says that all work done should be backed up within 24 hours, without any effort on the part of users. To achieve this, all work should be stored in the appropriate location on the server. Work that is stored on a server is backed up every day.

4.8.1 Use of memory sticks and transferring data

Memory sticks may be used, as long as they are encrypted devices approved and supplied by IT Services.

Under no circumstances must any RESTRICTED, confidential or sensitive data be copied to any form of removable media. If you're not sure then you must ask the Information Manager who can give advice on Data Protection issues.

Where RESTRICTED, Confidential or sensitive data needs to be sent outside the council, the preferred route would be via GCSx e-mail as this is certified to carry RESTRICTED data. If this is not possible then an alternative method of sending the data must be agreed and documented in consultation with IT Services.

4.8.2 Server room security

Since all of our corporate information is stored in the server room, it follows that this room should have additional physical security. The server room is a restricted area the door to it is kept locked, using a key-coded lock. The key code is changed regularly. The server room also houses an intrusion detection system this means that even if the main alarm is compromised, the server room alarm is still active.

In the event of a fire, the server room remains locked, however, it is possible to open the server room door from inside the server room without a key or key-code, so there is no risk to life.

All access to the server room must be logged in the server room access log detailing who, when and why access was required.

It is the responsibility of the Shared IT Services Manager to ensure that appropriate security controls are in place for the Server Room.

4.9 Data protection

Personal information on living individuals (who can be identified from the information held) that is stored on computers is subject to the Data Protection Act 1998. Compliance with the registration requirements of the Act is the responsibility of the Solicitor. Users must be aware of their responsibilities and further guidance is available from the Data Protection Officer. Users must inform the Data Protection Officer in writing of any proposals to keep personal information on a computer.

4.10 Compliance with the information security policy

The implementation of this policy will be reviewed regularly to ensure compliance. An audit of software and hardware will be conducted on a regular basis, as described above.

Any breach of this policy may lead to disciplinary action.

5.0 Review

This policy will be reviewed on a regular basis in the light of operating experience and/or changes in legislation.

Appendices to this document

Appendix A Authorised user agreement

Appendix B Password policy