BRIEFING NOTE

TO: Corporate Scrutiny and Performance Panel
DATE: 7 February 2008

RE: Information Security Policy Progress Update Briefing

Purpose

This high level briefing note has been written in response to an enquiry by the Corporate Scrutiny Panel to update them on the Council's current position regarding Information Security. Work had been initiated to review the existing data handling procedures following a request by ICT Cabinet Member and Executive Director after the loss of data by several Central Government Departments.

Background

Information Security is about protecting the confidentiality, integrity and availability of information assets. So this will include business continuity as well. Recent news reported the 'loss' of computer disks containing some 25 million personal records of adults and children in the UK by HM Revenue and Customs (HMRC) has raised awareness of information security within all private and public sector organisations across the country.

Walsall Council handles confidential information (including personal information) in a multitude of formats (including data on CDs, on the web, on USB drives, on paper etc) every day and it is easy to lapse into bad habits and just not 'think' about how confidential information should be managed.

Response/Action taken

The Council has had an Information Security Policy in place since January 2001. A copy of this policy is attached at Appendix 1 to this report. However, in light of the need for us all to be extra vigilant when handling confidential information, the Corporate Management Team (CMT) has taken the following action:

- After notification of the HMRC case, CMT re-issued the current Information Security Policy to staff, and re-quested Managers to discuss the potential risk exposure with regard to the capture, store, use and transfer of personal data within (and without) their teams. This request was made to all Executive and Assistant Directors on 14 December 2007 who were asked to cascade this information to their respective teams. A copy of the email is attached at Appendix 2 to this report;
- The instruction also prompted services to contact the ICT Service Desk for advice on any specific issues or data transfer they were unsure about;
- CMT have also requested that as the policy is 6 years old it should be reviewed in the light of new forms of technology and information sharing practices being used within the Council and its partners;
- A Project has been established to undertake this work and an external security consultant has been appointed to work with ICT to review and update the Policy. David Brown has taken on the role of Project Executive for this short piece of work;
- A revised Information Security Policy Statement (one A4 page) has been agreed and will be presented to CMT on 7th February for approval; and

- Following approval it will be issued to all staff – supported by an appropriate communication activity likely to include an email to all staff recommending their attention and a printed version to be within *all* payslips (to ensure those without easy email access are covered by the exercise).

It is important to note that the Information Security Policy Statement itself is only the beginning and should be viewed as the lead element in the Information Security Management System that needs to be "built" to support the ongoing maintenance of compliance with legislative, statutory and regulatory requirements with regard to the use, sharing and protection of information in the public sector.

With this in mind, the key activity of the current project phase is to identify the current gaps in relation to security compliance, benchmarking the Council against ISO 27001, the Information Security Management Standard. The scope of Information Security is incredibly broad, covering at minimum the following:

a) HR issues (reference checking, Acceptable Use policy compliance etc, user awareness training etc.)
b) Physical security issues - loss of laptops, data discs (!), destruction etc.
c) Information assets - what have you got, where is it stored, why, how long for, who has access to it - ditto, why, how long for; who do you share information with, how (encrypted or not?, discs or not? Paper or not?)

The intention is to ensure that the Information Security Policy Statement itself sits as the umbrella under which there is an Information Security Manual which documents and also signposts the supporting policies, standards, procedures and guidelines relevant to the organisation in order to provide evidence of the robust approach to ensure the protection of information as defined appropriate as the result of risk assessment. The best practice approach is *not* to be expending time, resource and budget on embedding controls for the sake of it but rather on the basis of evidence of the likelihood and impact of inadvertent disclosure/misuse/handling etc. This will be done in line with the existing council Risk Management Strategy.

Thus the steps for this project are identified below:

Step	Activity	Deliverable
1	*Determining the scope of the system* In order to provide an appropriate framework to move forward the compliance process. This activity defines the scope of the ISMS in terms of Council structure; Location; Assets; Technology.	*ISMS Scope*
2	*Prepare an Information Security Policy statement* to be available both internally and externally as required.	*ISP Statement*
3	*Review existing Gap Analysis* Covering all aspects described above based on the qualified assessment of suitability of the organisation's security management, documentary, procedural and control requirements which are to be in place for compliance with the standard.	*Gap Analysis review*
4	*Preparation of Security Improvement Programme* Recommendations will be made as to how shortfalls could be met, what improvements ought to be made, and what potential risk exposure exists, both current and residual	*Security Improvement Programme (SIP)*
5	*Identifying key information assets* To include review of existing physical asset registers and addition of relevant information assets – assisting in the	*Asset Register*

	creation of an appropriate Asset Register	
6	*Conducting an asset risk assessment (RA)* Assisting with risk assessment in terms of the current risks, threats and vulnerabilities using a bespoke 'round table' workshop methodology combined with documentation provided.	*Risk Assessment documentation (RA Standards, RA Procedure, RTP)*
7	*Developing a risk treatment plan (RTP)* This activity defines the organisation's approach to risk management in terms of: Scope of application; Risk analysis methodology; Technique of relating risks to countermeasures; Granularity of control options; Determination of assurance (Strength of Mechanism).	
8	*Developing a Statement of Applicability (SoA)* Produce Statement of Applicability corresponding to the applicable countermeasures required as a result of the Risk Assessment – referenced through the ISMS InfoSec Manual.	*Statement of Applicability (SoA)*
9	*Preparing a security manual, procedures and work instructions* This activity comprises the following parts: a) Produce the *core* operation and maintenance procedures, including record maintenance requirements – *certification deliverable*; b) Produce the Security Policy Manual consistent with the requirements of ISO27001 – *certification deliverable*.	*Security Policy*

The deliverables intended are described in more detail below:

Deliverables	
1.	A detailed **Gap Analysis Report** covering all aspects described above based on the qualified assessment of suitability of the organisation's security management, documentary, procedural and control requirements which are to be in place for compliance with the standard.
2.	Recommendations will be made as to how shortfalls could be met, what improvements ought to be made, and what potential risk exposure exists, both current and residual – in the form of a **Security Improvement Programme.**
3.	**Risk Treatment Plan** – required for Risk Assessment evidence in relation Code of Connection requirements and support for PCI DSS controls. In template form for future use.
4.	An agreed **Information Security Policy**
5.	A checklist of processes and systems required to support the policy and if already in place, assess their level of maturity (**Information Security Manual**).

The resultant Gap Analysis reports – together with a Security Improvement Plan (SIP) will be presented to CMT on 20th March.

Author
Paul Milmore – Head of ICT Strategy and Client Services
☎ 01922 655550
✉ milmorep@walsall.gov.uk

WALSALL METROPOLITAN BOROUGH COUNCIL

INFORMATION SECURITY POLICY

JANUARY 2001, VERSION 3

Angela K Cooke
Computer Consultant
Information Systems Services

Walsall Metropolitan Borough Council

CONTENTS

1. INTRODUCTION....5

2. WHAT IS INFORMATION SECURITY....5

3. COMPLIANCE....6

4. LEGISLATION....6

4.1 COPYRIGHT, DESIGNS AND PATENTS ACT 1988....6
4.2 COMPUTER MISUSE ACT 1990....6
4.3 DATA PROTECTION ACT 1998....6
4.4 ELECTRONIC COMMUNICATIONS ACT 2000....7
4.5 REGULATION OF INVESTIGATORY POWERS ACT 2000....7
4.6 THE TELECOMMUNICATIONS (LAWFUL BUSINESS PRACTICE) (INTERCEPTION OF COMMUNICATIONS) REGULATIONS....7
4.7 HUMAN RIGHTS ACT 1998....7

5. SECURITY EDUCATION....8

6. ASSET INVENTORY AND CLASSIFICATION....8

6.1 INVENTORY OF ASSETS....8
6.2 INFORMATION CLASSIFICATION....9

7. THE RISKS....9

7.1 CONFIDENTIALITY....9
7.2 INTEGRITY....10
7.3 AVAILABILITY....10
7.4 OTHER....11

8. PEOPLE SECURITY....11

8.1 TRAINING....11
8.2 CONFIDENTIALITY....11
8.3 TEMPORARY STAFF....11
8.4 OTHER ORGANISATIONS....11
8.5 SCREENING....12
8.6 LEAVERS....12
8.7 KNOWLEDGE....13
8.8 SEGREGATION OF DUTIES....13
8.9 INTERNET ACCESS POLICY....13
8.10 RESPONDING TO SECURITY INCIDENTS....13

9. PHYSICAL AND ENVIRONMENTAL SECURITY....14

9.1 SECURE AREAS....14
9.2 EQUIPMENT SECURITY....14
9.3 GENERAL CONTROLS....16

10. OPERATIONAL SECURITY....16

10.1 DOCUMENTED OPERATING PROCEDURES....16
10.2 CHANGE CONTROL....17
10.3 SEPARATION OF DEVELOPMENT AND OPERATIONAL FACILITIES....18
10.4 CAPACITY PLANNING....19

10.5 MALICIOUS SOFTWARE 19
10.6 INFORMATION BACKUP 20
10.7 SOFTWARE BACKUPS 20
10.8 OPERATIONAL LOGGING 20
10.9 MEDIA HANDLING 21
10.10 MEDIA DISPOSAL 21
10.11 INFORMATION HANDLING 22
10.12 SYSTEM DOCUMENTATION 22

11. COMMUNICATIONS SECURITY 22

11.1 NETWORK CONTROLS 22
11.2 INFORMATION EXCHANGE AGREEMENTS 23
11.3 MEDIA IN TRANSIT 24
11.4 LIMITED SERVICES 24
11.5 ENFORCED PATH 24
11.6 USER AUTHENTICATION FOR EXTERNAL CONNECTIONS 25
11.7 SEGREGATION IN NETWORKS 25
11.8 REMOTE DIAGNOSTIC PORT PROTECTION 25
11.9 NETWORK CONNECTION CONTROL 26
11.10 NETWORK ROUTING CONTROL 26

12. ACCESS CONTROL 26

12.1 PASSWORDS 26
12.2 UNATTENDED COMPUTER EQUIPMENT 27
12.3 SHARED COMPUTERS 27
12.4 SHARED INFORMATION 28
12.5 ACCESS AUTHORISATION 28
12.6 ACCESS REGISTER 29
12.7 LOG-ON PROCEDURES 29
12.8 USER IDENTIFICATION AND AUTHENTICATION 30
12.9 MONITORING 30
12.10 MOBILE COMPUTING AND TELEWORKING 31
12.11 ACCESS TO SYSTEM UTILITIES 32

13. BUSINESS CONTINUITY 32

13.1 THE NEED FOR BUSINESS CONTINUITY PLANNING 32
13.2 BUSINESS CONTINUITY MANAGEMENT PROCESS 33
13.3 WRITING AND IMPLEMENTING CONTINUITY PLANS 34
13.4 BUSINESS CONTINUITY PLANNING FRAMEWORK 34
13.5 TESTING, MAINTAINING AND RE-ASSESSING BUSINESS CONTINUITY PLANS 35

14. ROLES AND RESPONSIBILITIES 36

14.1 STRATEGIC EXECUTIVE TEAM 36
14.2 GENERAL AND SERVICE MANAGERS 36
14.3 SYSTEM ADMINISTRATORS 37
14.4 INDIVIDUALS 37
14.5 INTERNAL AUDIT 38
14.6 INFORMATION SYSTEMS SERVICES 38

15. E-GOVERNMENT AND E-COMMERCE 39

15.1 PUBLISHING INFORMATION ON THE INTERNET 39

15.2 COLLECTING INFORMATION VIA THE INTERNET 39
15.3 E-TRANSACTIONS WITH A CUSTOMER 39
15.4 BUYING VIA THE INTERNET (E-PROCUREMENT) 40
15.5 M-BUSINESS 41

16. FURTHER READING AND GUIDELINES 41

APPENDIX 1 – ANTI-VIRUS PROCEDURES 42

Precautions to be Taken Against Virus Attack 42
What to do if you get a virus 42

APPENDIX 2 – SECURITY STANDARDS SPECIFIC TO THE VME OPERATING SYSTEM 43

1. Introduction

The purpose of this document is to document the Council's information security standards. The policy covers, in detail, the actions required of the Information Systems Services Division, Internal Audit, senior managers, system administrators and individual members of staff in order to comply with the Information Security Policy and associated English and European law.

This version of the Information Security Policy (The Policy) supersedes the Computer Security Policy, published in 1996. The Policy follows the guidelines recommended in BS 7799-1:1999, the British Standard for Information Security Management.

A copy of this document will be held in each Service Area of the Authority and at each work place. Summary versions, detailing the responsibility of the individual will be sent to all staff. A copy of the summary will be sent to new starters before they commence work at the Authority. Additional copies of the summary version can be obtained from the Customer Service Desk (Extension 2862).

This Security Policy is intended to apply to all information, electronic and manual, within the Council.

2. What is Information Security

Information is an asset which, like other important business assets, has value to the Council (in fact the Council could not operate without it) and consequently needs to be suitably protected. Information security protects information from a wide variety of threats in order to ensure business continuity, minimise damage, and maximise scarce resources.

Information can exist in a variety of forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films or spoken in conversation.

Information security is characterised here as the preservation of:

- Confidentiality: ensuring that information is accessible only to those authorised to have access;
- Integrity: safeguarding the accuracy and completeness of information and processing methods;
- Availability: ensuring that authorised users have access to information and associated assets when required.

Information security is achieved by implementing a suitable set of controls, which can be policies, practices, organisational structures and software functions (or any combination of such). The controls need to be established to ensure that the specific security objectives (confidentiality, integrity, availability) of the Council are met.

3. Compliance

This Policy is the Council's Information Security Policy, and as such, has approval from the Strategic Executive Team. Failure by a Council Officer to comply with the Policy may result in disciplinary action (not excluding dismissal) in accordance with the Council's Disciplinary Procedures.

The Council will, when circumstances warrant, monitor the use and content of e-mail, and Internet access by its' employees. The Council will, when circumstances warrant, carry out surveillance of its employees in accordance with the Council's Surveillance Protocol.

4. Legislation

Various legislation affects information security. This Policy is not intended to give detailed information about the legislation. In some cases, further information on specific legislation is available.

4.1 Copyright, Designs and Patents Act 1988

This Act covers software, screensavers, documents, music, videos, etc. It is unlawful to copy copyright protected material without the copyright owner's permission. The penalties for infringing this Act include unlimited fines and up to two years in prison. The penalties can apply to the individual who committed the offence and to his/her manager. Ignorance of the law is not a defence.

It is the policy of this Council to purchase licences for all copies of software (or other copyright protected material). No employee of the Council is authorised to use or load software, or other material, onto the Council's computer equipment that has not been lawfully purchased.

4.2 Computer Misuse Act 1990

This Act is mainly concerned with "hacking", i.e. the unauthorised access to a computer, usually via a telephone line. The Act, however, also covers unauthorised access by anybody, by any method, for any reason. This includes the Council's employees gaining unauthorised access to any of the Council's computers, or using those computers for an unauthorised purpose.

A person convicted under this Act can be sentenced to up to five years in prison or fined.

4.3 Data Protection Act 1998

This Act covers the processing of personal data (that is, any information about an identifiable living individual). Any Council employee who has any contact with personal data must be

aware of how the Act affects them. Detailed guidelines can be found in Exchange, All Public Folders, Council Information, Strategy Documents, Data Protection Act 1998 folder, WMBC Guidelines.

4.4 Electronic Communications Act 2000

The aim of this Act is to facilitate electronic commerce. The Act provides for the admissibility of electronic signatures and related certificates in legal proceedings. Electronic signatures are now admissible as evidence in respect of any question regarding authenticity or integrity of an electronic communication or data.

The Act does not yet cover instances whereby other legislation states that documentation must be authorised by a written signature or must be on paper. Secondary legislation will be produced over time to amend existing legislation to allow electronic storage or communication.

4.5 Regulation of Investigatory Powers Act 2000

This Act lays down the procedures and conditions under which communications (electronic or otherwise) can be intercepted. This includes the interception of email, telephone conversations, mail, etc. It should not affect the Council unless the Police (or other authorised body) produce a warrant to intercept communications using our telephone network or e-mail. However, we are under an obligation to provide information once such a warrant has been produced.

4.6 The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations

This legislation allows organisations to monitor their own computer and telephony networks.

4.7 Human Rights Act 1998

Information security measures may, in some instances, impinge on an individual's human rights under this act. The article most likely to cause problems (but not the only one) is Article 8 – "everyone has the right to respect for his private and family life, his home and his correspondence". To make sure that the Council does not fall foul of this Act, the Council must comply with the rest of English law that applies. If the Council does so comply, then it is the Law that is wrong and not the Council.

To avoid infringing an individual's privacy rights when using CCTV, the Council will adhere to the Information Commissioner's CCTV Code of Practice. Compliance with the forthcoming Employment Code of Practice – use of personal data in employer/employee relationships (also from the Information Commissioner) will also be required when planning surveillance (covert or overt) of employees.

5. Security Education

All staff who have any sort of access to any of the Council's information must be aware of their responsibility under this Policy.

- Security should be addressed at the recruitment stage and included in individual job descriptions.
- Users must be trained in security and the correct use of IT facilities. The training should ensure that they are aware of security threats and concerns and that they are equipped to support the Information Security Policy in the course of their normal work.
- All employees must be made aware of the procedures for reporting security incidents and be required to report such incidents immediately to the appropriate manager or Internal Audit.
- Staff with vital skills must be identified and consideration given to the action necessary should they leave. It is not desirable to have one individual with unique and vital skills, if only to guard against their holiday periods and absences.

6. Asset Inventory and Classification

6.1 Inventory of Assets

Inventories of assets help ensure that effective asset protection takes place. The process of compiling an inventory of assets is an important aspect of risk management. Each service area must maintain an inventory of all assets associated with its' information. Based on this information, the service area can then provide levels of security appropriate to the value and importance of the asset. Each asset should be clearly identified and its ownership, current location and security classification (see 6.2) agreed and documented. Examples of assets associated with information are as follows:

a) Information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information;
b) Software assets: application software, development tools and utilities;
c) Physical assets: computer equipment (processors, monitors, laptops, modems), communications equipment (routers, PABXs, fax machines, answering machines), magnetic media (tapes and disks), other technical equipment (power supplies, air conditioning units), furniture, accommodation;
d) Services: computing and communications services, general utilities, e.g. heating, lighting, power, air conditioning.

6.2 Information Classification

Information is an asset, and as such should be inventoried and must be classified. Information has varying degrees of sensitivity and criticality; the classification must cater for this. The level of security required will depend on the classification level. The Council's classification levels are given in the following table:

Security Level	Description
0	Public information
1	Where disclosure to unauthorised persons would be inappropriate or inconvenient
2	Where disclosure to unauthorised persons would cause significant harm to the Council (financial loss, embarrassment or loss of reputation, damage or distress to an individual or another organisation).
3	Where disclosure to unauthorised persons would cause serious harm to the Council (serious financial loss, grave embarrassment or loss of reputation, severe damage or distress to an individual or another organisation).

The security level of information is not static, for example, a committee report may be at level 1 during its' draft stage, but would go to level 0 once it was released to the press.

All information sets should be labelled with a security level.

7. The Risks

7.1 Confidentiality

Confidentiality can be compromised deliberately or accidentally. Deliberate attempts to compromise confidentiality are generally rare, some examples follow:

- Hacking;
- Misuse by a Council officer;
- Theft (now quite common – when a PC or laptop is stolen, the information goes with it).

Accidental breaches of confidentiality are more common - inadequate staff training and carelessness are the main causes of this, for example:

- Leaving papers lying around where unauthorised people may see them;

- Staff trying to be helpful can disclose confidential information to unauthorised people because they are not aware of procedures.

7.2 Integrity

Information can get corrupted in a variety of ways. Some corruptions are obvious (e.g. when the whole file shows "gobbledygook"), others are not so obvious (e.g. a spreadsheet may have erroneous figures in it, or a report may have the wrong facts or dates, etc.). Integrity can be compromised deliberately or accidentally. Examples of deliberate or malicious activities that can cause corruption are as follows:

- Computer virus infection;
- Fraudulent activities;
- Hacking.

Examples of accidental activities that can cause corruption are as follows:

- Typing errors;
- Untrained staff;
- Hardware failure;
- Incompatible software;
- Power cuts.

7.3 Availability

Tight security can be seen as a hindrance to availability – a document sealed in a watertight canister that is dropped into the deepest part of the Pacific Ocean would be secure. However, it would not be very easy to access the information when required! There needs to be a balance between keeping information confidential and accurate, and enabling authorised users to access the information.

Problems with availability can be caused deliberately or accidentally. Examples of deliberate actions aimed at causing unavailability are:

- Theft;
- Vandalism;
- Denial of service attacks.

Examples of what can accidentally cause unavailability are:

- Loss of papers;
- Untrained staff;
- Network overload;
- "Disaster";

- Equipment failure;
- Power cuts.

7.4 Other

Illegal copying of software puts the Council at risk from litigation by such organisations as the Federation Against Software Theft (FAST) and the American equivalent – the BSA. Illegal copies of software also carry a high risk of virus infection and corruption.

The Internet poses several risks to the Council's operation – not all of them to do with security of information. The risks from the Internet to information security are given above, other risks include time wasting ("cyber-skiving") and litigation against the Council if a member of staff downloads illegal or unsuitable material.

8. People Security

8.1 Training

All staff must be trained in security procedures, security requirements, legal responsibilities, etc. They must also be trained in the correct use of the information processing facilities (e.g. log-on procedures, use of software packages, etc.) appropriate for their job. Training must be complete before access to information or services is granted.

8.2 Confidentiality

The Code of Conduct for Council Employees has a section on confidentiality. All staff must be aware of and abide by this. All staff must also be aware of which information they have access to is covered by a duty of confidence.

8.3 Temporary Staff

Temporary staff, contractors, work experience people, etc. must not be given access to any of the Council's information which is classified at security level 1,2 or 3 without signing a confidentiality agreement. All such staff must also receive proper training (security and job related) appropriate to the work they will be doing for the Council. Any temporary staff who have access to information classified as security level 2 or 3, must be closely monitored.

Do not let temporary staff have unsupervised access to the Internet.

8.4 Other Organisations

Where the Council's partners or other organisations contracted to the Council, are to be given access to Council information classified at level 1, 2 or 3, there must be a formal agreement addressing information security issues between the parties.

8.5 Screening

Verification checks on permanent staff should be carried out at the time of job applications. This should include the following:

a) Availability of satisfactory character references;
b) A check (for completeness and accuracy) of the application form;
c) Confirmation of claimed academic and professional qualifications;
d) Independent identity check (passport or similar document).

Where a job, either on initial appointment or on promotion or transfer, involves the person having access to information processing facilities, and in particular if they are handling information classified as security level 2 or 3, the Council should also carry out a credit check. For staff holding positions of considerable authority this check should be repeated annually.

A similar screening process should be carried out for contractors and temporary staff. Where these staff are provided through an agency the contract with the agency should clearly specify the agency's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern.

General and service managers should evaluate the supervision required for new and inexperienced staff with authorisation to access sensitive systems.

General and service managers should be aware that personal circumstances of their staff might affect their work. Personal or financial problems, changes in their behaviour or lifestyle, recurring absences and evidence of stress or depression might lead to fraud, theft, error or other security implications.

8.6 Leavers

Once a member of staff has handed in his/her notice, then every attempt must be made to ensure that the Council's information systems do not suffer. The outgoing member of staff must ensure that there is enough documentation to enable the work to carry on without him/her. If possible, the person who will take over the work should be trained in his/her new duties before the outgoing officer leaves. The outgoing officer must also ensure that his/her mailbox is emptied.

As soon as a member of staff leaves, all his/her user names and permissions to information systems should be deleted – at the very least the password(s) must be changed. Any mailboxes belonging to the officer must be deleted.

Additional monitoring should be applied to officers who access the Council's information whilst serving out their notice. Those officers dismissed for disciplinary reasons who are serving their notice, or officers suspended pending a disciplinary investigation, should not be allowed access to any of the Council's information unless it is absolutely necessary.

8.7 Knowledge

Avoid situations where only one person knows anything about an information system or data set. Where problems would occur if that person's knowledge were not available (short or long term, or never again), backup that person's knowledge with very good documentation and by training other officers. Do not wait until the officer with the knowledge leaves or goes on long-term sickness.

8.8 Segregation of Duties

Duties should be segregated to minimise the risk of negligent or deliberate system misuse and consideration should be given to separating the management or execution of certain duties, or of areas of responsibility, in order to reduce opportunities for unauthorised modification or misuse of data or services. In particular, the same employees should not carry out the following functions:

- business system use;
- data entry;
- computer operation;
- network management;
- system administration;
- systems development and maintenance;
- change management;
- security administration;
- security audit.

8.9 Internet Access Policy

All employees who wish to use the Council's Internet and external e-mail facilities, or to access their internal mail from external equipment, must read, and comply with, the Council's Internet Access Policy. No officer will be given permission to use these facilities without formal authorisation by a general or service manager. A copy of the Internet Access Policy and an application form can be found in the All Public Folders, Council Information, Council Guidelines folder.

8.10 Responding to Security Incidents

Internal Audit must be informed of all actual or suspected security breaches. Any officer spotting any irregularities must inform the appropriate manager, who should then inform Internal

Audit. Internal Audit, as well as investigating and resolving the breach, keep a central log of all such incidents.

Any observed or suspected security weaknesses or malfunctions in computer software must be reported to the appropriate manager and to the software supplier. In some instances, ISS should also be notified. Any such weaknesses in manual procedures should be reported to the appropriate manager. Those responsible for the information that the weakness puts at risk, must establish procedures to either cure the weakness or to provide a work around.

9. Physical and Environmental Security

9.1 Secure Areas

Information should be held in secure areas. The security level of the information determines how much security is necessary. Areas such as the central computer room must have the highest security against environmental and physical damage to equipment. Access must be limited to authorised personnel only and arrangements made to ensure that any unauthorised personnel are always supervised when making necessary visits (e.g. engineers). If an authorised officer becomes unauthorised (e.g. when s/he changes duties or leaves the Council), any keys must be reclaimed and keypad numbers, etc. changed when the officer finishes his/her duties. Hazardous or combustible materials should not be stored in these areas and proper fire prevention facilities must be in place.

Information held outside computer rooms must still be protected. All unattended offices must be kept locked and windows closed. External protection should be considered for windows, particularly at ground level. Suitable intruder detection systems (regularly tested) must be installed for those areas most at risk from burglary. CCTV can be used to deter theft or to catch offenders, however, if CCTV is to be used, the procedures used must comply with the Information Commissioner's CCTV Code of Practice (see All Public Folders, Council Information, Strategy Documents, Data Protection Act 1998). Paper documents must not be left lying around unless the information concerned is in the public domain. Information classified as security level 2 or 3 must be locked away when not in use.

Fall back equipment and backup media should be sited at a safe distance to avoid damage from a disaster at the main site.

9.2 Equipment Security

a) **Equipment Siting and Protection.** Equipment (computers, printers, fax machines, photocopiers, etc.) should be sited or protected to reduce risks from environmental threats and

hazards and opportunities for unauthorised access. Consider ways of preventing or minimising the effects of the following:

- Unauthorised staff seeing information as they walk past;
- Theft;
- Fire;
- Explosives;
- Smoke;
- Water (or supply failure);
- Dust;
- Vibration;
- Chemical effects;
- Electrical supply interference;
- Electromagnetic radiation.

Make special arrangements if there is a requirement to receive or send a fax containing sensitive information (e.g. a medical report on a member of staff) to a fax machine in an open office.

b) **Power Supplies.** All servers must be protected by uninterruptible power supply (UPS) equipment and software. In the event of a power failure, this equipment and software will automatically close the server down properly. The mainframe must have an emergency power switch located near the emergency exit for rapid close down in the event of an emergency. Lightning protection should be applied to all buildings and lightning protection filters should be fitted to all external communication lines.

c) **Cabling Security.** Power and telecommunications lines into information processing facilities should be underground where possible, or subject to adequate alternate protection. Building maintenance personnel should know where the cables are before performing any operation that would put the cabling at risk (e.g. drilling holes in walls). Power cables should be segregated from communications cables to prevent interference.

d) **Equipment Maintenance.** Equipment should be correctly maintained to ensure its continued availability and integrity. It should be maintained in accordance with the supplier's recommended service intervals and specifications. Only authorised people can carry out repairs on and service equipment. Records will be kept of all suspected or actual faults and all preventative and corrective maintenance undertaken. When equipment has to be sent or taken off-site

for repair, any information held on the equipment must be deleted. If the information is security level 2 or 3, the information must be overwritten before the equipment goes off-site.

e) **Equipment Off-site.** Equipment (laptops, etc.) and media (papers, etc.) taken off-site must not be left unattended in public places. Suitable precautions must be taken by an officer to prevent theft of the equipment from either home or car. Laptops should be carried as hand luggage and disguised where possible. They should not be left in cars in public car parks, on street parking, or left in view from the street outside the house, etc. PCs should not be used at home for business activities if virus controls are not in place. Portable PCs should be provided with an appropriate form of access protection (e.g. password or encryption) to prevent unauthorised access to their contents in the event of loss or theft.

f) **Disposal or Re-use of Equipment.** Information can be compromised through careless disposal or re-use of equipment. Storage devices containing security level 2 or 3 information should be physically destroyed or overwritten rather than using the standard delete function.

9.3 General Controls

Papers and removable storage media (CD's, floppy disks, DVD's, etc.) left out on desks are at risk from theft, unauthorised access, fire and flood damage, etc. Such items must be stored in lockable cabinets or drawers when not in use, particularly outside working hours. Sensitive or critical information should be locked away in a fire proof safe or cabinet.

Computers must never be left "logged in" outside working hours. During working hours, password protected screensavers must be activated when a computer is left unattended.

Security level 2 or 3 information, when printed or photocopied, must be removed from printers or photocopiers immediately – unless the equipment is in a secure computer room.

10. Operational Security

10.1 Documented Operating Procedures

All operating procedures must be documented in such a way that if the officer who normally performs the backup, data transfer, closedown, etc. is unavailable, then somebody else will be able to run the procedures without difficulty.

The procedures should give detailed instructions for jobs such as:

- Processing and handling information;
- Scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;
- Handling of errors or other exceptional conditions;
- Contact details in the event of operational or technical difficulties;
- Any special output handling instructions;
- System restart and recovery and when to use them.

10.2 Change Control

a) Changes to Software and/or Equipment. Changes to computer systems and equipment must be controlled, as inadequate control is often the cause of system or security failures. Formal management responsibilities are necessary to ensure satisfactory control of all changes to equipment, software or procedures. In particular, the following items should be covered:

- Identification and recording of significant changes;
- Assessment of the impact of such changes;
- Approval procedure for the proposed changes;
- Communication of change details to all relevant persons;
- Procedures and responsibilities for aborting and recovering from unsuccessful changes.

Procedures for changes to software should cover the following additional items:

- A record of those persons authorised to request changes, accept proposals, and accept the change when implemented. The record should also include the IT team focal point for change requests;
- Only accepting changes submitted by authorised users;
- Reviewing security controls and integrity procedures to ensure they will not be compromised by the change;
- Identifying all computer software, data files, database entities, and hardware that require amendment;
- Obtaining approval for detailed proposals before work commences;
- Ensuring that changes are accepted by the authorised user before implementation;
- Ensuring that system documentation is updated on completion of each change, and that old documentation is archived or disposed of;

- Maintaining a version control for all software updates;
- Maintaining an audit log of change requests.

b) Operating System Changes. Periodically, operating system vendors issue new releases of their software. When changes occur, the application system must be reviewed to ensure that there is no adverse impact on security. This process should include:

- Review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes;
- Ensuring that notification of operating system changes are provided in time to allow appropriate reviews to take place before implementation.

When operating system vendors issue security patches for software, these patches must be evaluated and applied within as short a time as possible.

When installing operating systems, all default settings must be checked to make sure they suit the circumstances. Default passwords must always be changed.

c) Changes to Software Packages. Modifications to software packages must be discouraged. As far as possible, and practicable, vendor supplied software should be used without modification. In circumstances where it is deemed essential to modify a package, the following points must be considered:

- The risk of built-in controls being compromised;
- The possible need to obtain the consent of the vendor;
- The possibility of obtaining the required changes from the vendor as standard program updates;
- The possibility of the Council becoming responsible for the future maintenance of the software as a result of changes.

If changes are essential, then the original software must be retained and the changes applied to a clearly identified copy. These changes should be fully documented, to allow them to be re-applied if necessary to future software updates.

10.3 Separation of Development and Operational Facilities
Operational software and data must be kept separate from development and testing facilities. In particular the following controls must be considered:

- Development and operational software should, where possible, run on different computer processors, or in different domains or directories.
- Development and testing activities should be separated as far as possible.
- Compilers, editors and other system utilities should not be accessible from operational systems when not required.
- Development staff should only have access to operational passwords where controls are in place for issuing passwords for the support of operational systems. Controls must ensure that such passwords are changed after use.

10.4 Capacity Planning

Capacity demands must be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available. These projections must take account of new business and system requirements and current and projected trends in the Council's information processing. Managers must use this information to identify and avoid potential bottlenecks that might present a threat to security or user services, and plan appropriate remedial action. For example, security could be compromised if confidential or sensitive documents were left lying on desks just because there was no lockable storage space for them.

10.5 Malicious Software

Viruses pose a real threat to the Council's PCs and servers. A virus is an undesirable piece of software that corrupts the data of a computer's hard disk. They are written by malicious individuals and introduced to a computer either through a network, via an e-mail or via a corrupted floppy disk or CD/DVD.

All Council PC's must have the latest version of the Council's approved virus checking software installed. Procedures for installing updates to the software can be found on the Council's Intranet (under "Computer Related") and in All Public Folders, Hot News, McAfee TVD Software folders.

All non-Council owned PC's which log into the Council's network must have an ISS approved up to date virus checker installed.

Games software is a notorious for the spread of viruses. Games must not be loaded onto the Council PCs.

Virus checkers are not the universal panacea that their suppliers would have us believe. New viruses are surfacing everyday, and a virus checker update is out of date as soon as it is released. General precautions that all Council officers must take, and

instructions on how to deal with an infection are given in Appendix A.

10.6 Information Backup

Information must be backed up at regular intervals. Back up copies must be afforded the same security cover as the original information. Information recorded on the Council's mainframe computer and central servers is automatically backed up every night. These back ups are stored in a fireproof safe. Once a week, a backup copy of the information is removed to off-site storage.

It is the responsibility of the information owner to back up information held locally on PCs'. Such information must be backed up at least weekly (daily if possible), and the back up copies stored safely. Important data should have an off-site backup.

Information stored on paper or other non-electronic media should also be backed up.

10.7 Software Backups

Mainframe software is backed up regularly. Tailored or specialist software on servers or PC's should be backed up when first installed and after any changes. The two last backups should be retained.

10.8 Operational Logging

Operational staff must maintain a log of their activities. Logs should include, as appropriate:

- System start and finish times;
- System errors and corrective action taken;
- Confirmation of the correct handling of data files and computer output;
- The name of the person making the log entry.

Operator logs must be subject to regular, independent checks against operating procedures.

Faults must be reported and corrective action taken. Faults reported by users regarding information processing or communications systems must be logged. The rules for handling reported faults include:

- Review of fault logs to ensure that faults have been satisfactorily resolved;
- Review of corrective measures to ensure that controls have not been compromised, and that action taken is fully authorised.

10.9 Media Handling

Procedures for handling media such as tapes, disks, cassettes and printed reports, etc. must consider:

- What should happen to the previous contents of re-usable media, once those contents are no longer required. Should they be erased or over written?
- What authorisation is required before the media is removed from the Council and whether a record or audit trail is required of such removals;
- All media must be stored in a safe, secure environment in accordance with manufacturers' specifications;
- All procedures and authorisation levels must be clearly documented.

10.10 Media Disposal

Media must be disposed of securely and safely when no longer required. Formal procedures for the secure disposal of media must be established to minimise the risk. A recent example was the discovery of medical records in a skip outside of a supermarket! Examples of media that might require secure disposal are as follows:

- Paper documents;
- Microfiche;
- Voice or video recordings;
- Carbon paper;
- Magnetic tapes or cartridges
- Removable disks or diskettes, CDs, DVDs;
- Program listings;
- Test data
- System documentation.

When setting up procedures for secure disposal of media, the following guidelines must be considered:

- Media containing sensitive information (classified at security level 2 or 3) must be stored securely and safely disposed of, e.g. by incineration or shredding, or emptied of data/overwritten for use by another application;
- It may be easier to arrange for all media items to be securely disposed of, rather than attempting to separate out the sensitive items;
- If a contractor is used to dispose of media, make sure the contract includes appropriate security measures;
- Disposal of sensitive items (those classified at security level 2 or 3) should be logged, where possible, to maintain an audit trail.

10.11 Information Handling

Procedures for the handling and storage of information must be established in order to protect such information from unauthorised disclosure or misuse. Procedures must be drawn up for handling information which are consistent with its security classification in documents, computing systems, networks, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities, use of fax machines and any other sensitive items, e.g. blank cheques, invoices. The following items must be considered when drawing up these procedures:

- Handling and labelling of all media;
- Access restrictions to identify unauthorised personnel;
- Maintenance of a formal record of the authorised recipients of data;
- Ensuring that input data is complete, that processing is properly completed and that output validation is completed;
- Protection of spooled data awaiting output to a level consistent with its' sensitivity;
- Storage of media in an environment which accords with the manufacturer's specification;
- Keeping the distribution of information to a minimum;
- Clear marking of all copies of data for the attention of the authorised recipient;
- Review of distribution lists and lists of authorised recipients at regular intervals.

10.12 System Documentation

System documentation can give an unauthorised person the knowledge to access information systems they should not have access to. The following controls must be considered to protect system documentation from unauthorised access:

- System documentation should be stored securely;
- The access list for system documentation must be kept to a minimum and authorised by the system owner;
- System documentation held on a public network or supplied via a public network should be appropriately protected.

11. Communications Security

11.1 Network Controls

A range of network controls is required to achieve and maintain security in computer networks. Network administrators must implement and maintain controls to ensure the security of data in networks, and the protection of connected services from

unauthorised access. In particular the following items must be considered:

- Operational responsibility for networks should be separated from computer operations where appropriate;
- Responsibilities and procedures for the management of remote equipment, including equipment for user areas, should be established;
- Special controls must be established to safeguard the confidentiality and integrity of data passing over public networks and to protect connected systems;
- Special controls may be required to maintain the availability of the network services and computers connected.

11.2 Information Exchange Agreements

Agreements, where appropriate, must be established for the exchange of information with other organisations. In some instances (e.g. whereby an organisation processes personal data on the Council's behalf), there must be a formal contract in place. Formal information sharing protocols are required when regular sharing of information occurs between the Council and other organisations. All such agreements must include security provisions for the information. What security measures are required will depend on the security classification of the data, but the following must be considered:

- Management responsibilities for controlling and notifying transmission, despatch and receipt;
- Procedures for notifying sender, transmission, despatch and receipt;
- Minimum technical standards for packaging and transmission;
- Courier identification standards;
- Responsibilities and liabilities in the event of the loss of data;
- Use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected;
- Information ownership responsibilities for data protection and similar considerations;
- Technical standards for recording and reading information;
- Any special controls that may be required to protect sensitive items, such as cryptographic leys.

11.3 Media in Transit

Information can be vulnerable to unauthorised access, misuse, damage or corruption during physical transport, for instance when sending information via the postal service or via courier. The following controls must be considered, and applied where necessary, before transporting information:

- Reliable transport or couriers should be used. A list of authorised couriers should be agreed by management and a procedure to check the identification of the couriers implemented;
- Packaging should be sufficient to protect the contents from any physical damage likely to arise during transport and in accordance with the manufacturers' specifications.

Extra precautions may be required to protect sensitive information in transit, for example:

- Use of locked containers;
- Delivery by hand;
- Tamper-evident packaging (which reveals any attempt to gain access);
- In exceptional cases, splitting the consignment into more than one delivery and despatch by different routes.

11.4 Limited Services

Users will only be allowed access to the services, software and files that they are authorised to use.

11.5 Enforced Path

Where appropriate, the route from the user terminal or PC will be controlled by creating an enforced path. This will prevent accidental or deliberate straying of users into parts of the network that they are not authorised to access. The path may be enforced in a variety of ways as follows:

- Allocating dedicated lines or telephone numbers;
- Automatically connecting ports to specified application systems or security gateways;
- Limiting menu options for individual users;
- Preventing unlimited network "roaming";
- Enforcing the use of specified application systems and/or security gateways for external network users;
- Actively controlling allowed source to destination communications via security gateways such as firewalls;
- Restricting network access by setting up logical domains, e.g. virtual private networks, for user groups within the Council.

11.6 User Authentication for External Connections

External connections provide a potential for unauthorised access to Council information. Therefore, access by remote users must be subject to authentication. It is important to determine from a risk assessment the level of protection required. Examples of methods of authentication are as follows:

- Cryptographic based techniques;
- Hardware tokens;
- Challenge/response protocol;
- Dedicated private lines;
- Network user address checking;
- Dial back procedures.

When using dial back procedures and controls, network services that include call forwarding must not be used. It is also important that the call back process includes ensuring that an actual disconnection on the Council's side occurs.

11.7 Segregation in Networks

Networks are increasingly being extended beyond traditional boundaries, as partnerships with other organisations are formed which require the interconnection or sharing of information processing and networking facilities. Such extensions will increase the risk of unauthorised access to already existing networked systems. Some of these systems will require protection from other network users because of their sensitivity or criticality.

One method of controlling the security of large networks is to divide them into separate logical domains, each protected by a defined security perimeter. Such a perimeter can be implemented by installing a secure gateway between the two domains to be interconnected to control access and information flow between the two. This gateway must be configured to filter traffic between the domains and to block unauthorised access. An example of this type of gateway is what is commonly referred to as a firewall.

Risk assessment must be used to balance the security threats against the relative cost and performance impact of incorporating suitable network routing or gateway technology.

11.8 Remote Diagnostic Port Protection

Access to diagnostic ports used by external hardware/software support personnel must be securely controlled. Similarly, remote access for support purposes by Council staff (usually ISS) must only be granted with the consent of the system owner.

11.9 Network Connection Control

Where there is a requirement to link to other, external networks, controls can be implemented through network gateways that filter traffic by means of pre-defined tables or rules. Restrictions can be applied as follows:

- Electronic mail only;
- One-way file transfer;
- Two-way file transfer;
- Interactive access;
- Network access linked to time of day or date.

11.10 Network Routing Control

Shared networks, especially those extending outside the Council, may require the incorporation of routing controls to ensure that computer connections and information flows are safe from unauthorised access.

Routing controls should be based on positive source and destination address checking mechanisms. Network address translation is also useful for isolating networks.

12. Access Control

12.1 Passwords

There are several rules regarding passwords that must be adhered to, especially if that password would give access to sensitive, personal or critical data, as follows:

- Keep passwords confidential, do not share them with anyone;
- Avoid keeping a paper record of passwords, unless this can be stored securely;
- Change passwords whenever there is any indication of possible system or password compromise;
- Change passwords at regular intervals (passwords for privileged users should be changed more frequently than normal passwords), and avoid re-using or cycling old passwords;
- Do not use common words or mnemonics (e.g. PASSWORD, FRED, your initials, your date of birth, etc.). It is best not to use any word found in a dictionary or proper nouns;
- Use at least six characters for your password – preferably eight;
- Keep the password free of consecutive identical characters or all-numeric or all-alphabetic groups;
- Make the password easy to remember;
- Do not re-use, or cycle, old passwords;
- Each individual user should have a personal password;

- Change temporary passwords at the first log-on;
- Do not include passwords in any automated log-on process, e.g. stored in a macro or function key;
- ALWAYS change default passwords when installing new software;
- Do not allow anybody to overlook the keyboard whilst typing in a password.

One suggestion is to use the initials from a song or book title and include a special character (i.e. anything that is not alphabetic or numeric, e.g. *&£@/) randomly within the password.

Where possible, software should be used to enforce the above rules. The software should also:

- Allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;
- Not display passwords on the screen when being entered;
- Store passwords separately from application system data;
- Store passwords in encrypted form using a one-way encryption algorithm.

12.2 Unattended Computer Equipment

Users should ensure that unattended equipment has appropriate protection for the information held on that equipment. The hard disk of any PC, without additional security, can be accessed by anybody. To access the Council's network, a user name and password is required. Users must, when temporarily leaving their PC's unattended:

- Activate a password protected screen saver;
- Log-off mainframe computers when the session is finished.

Users must log out of all systems and networks and switch off their PCs when leaving them unattended overnight.

Sensitive, personal or confidential data must not be left on an unattended PC without additional protection to that supplied as standard.

12.3 Shared Computers

If a computer is shared, each individual must have his or her own log on and password. When one person finishes a session, s/he must log out before another person logs on.

12.4 Shared Information

Information held on individual Windows machines can be shared with other Windows machines. This facility can be very useful, but shares must only be set up where there is a true requirement, and must always be revoked when the need is over.

12.5 Access Authorisation

All information must have an “owner” who is responsible for (sometimes on instructions from management) authorising access to that information. The information may be paper files or individual documents on a PC, as well as major corporate databases and systems on the mainframe and servers.

Owners of shared systems on the mainframe and servers must allocate an officer as a system administrator, who is responsible for authorising access to their system(s). In some cases, individual users will require formal authorisation from management to gain access.

Who should be given access to systems and information, and also what type of access (e.g. read only) must be decided on the basis of “need”. For instance, everybody has a legal right to view public committee minutes, but only a very few can create or amend them – nobody can delete them.

Each appropriate system must have a set of rules to determine who should have what access. How restrictive these rules are will depend on the security classification of the information held by the system. Ultimate responsibility for these rules lies with General and Service Managers, in some cases implementing strategies set by the Strategic Executive Team. Responsibility for implementing the rules is usually delegated to the system administrator. Blanket permissions to access information must be avoided, except in very rare cases. Each individual user must be assessed against the rules and granted permission accordingly.

Once an individual has been allocated access permissions, those permissions must be reviewed regularly (at least once every six months). If a person changes his/her job or responsibilities, then his/her permissions must be altered accordingly. As soon as an officer leaves the Council, his/her permissions must be revoked immediately.

Printed output from applications systems handling sensitive information must only contain information that is relevant to the purpose of the output. The output must only be sent to authorised printers, locations, or people.

12.6 Access Register

There must be a formal user registration and de-registration procedure for granting access to multi-user information systems and services. The procedure should include:

- Using unique user identifiers so that users can be linked to and made responsible for their actions. The use of group identifiers should only be permitted when they are suitable for the work carried out;
- Checking the user has permission from the system owner for the use of the information system or service. Separate approval for access rights from management may also be appropriate;
- Checking the level of access granted is appropriate to the business purpose and is consistent with this Security Policy, e.g. it does not compromise segregation of duties;
- Giving users a written statement of their access rights;
- Requiring users to sign statements indicating that they understand the conditions of access;
- Ensuring service providers do not grant access until authorisation procedures are completed;
- Maintaining a formal record of all persons registered to use the service;
- Immediately removing access rights of users who have changed jobs or left the Council;
- Periodically checking for, and removing, redundant user identifiers and accounts;
- Ensuring that redundant user identifiers and accounts are not issued to other users.

12.7 Log-on Procedures

Access to information systems should be via a secure log-on process. The procedure for logging on to a computer system should be designed to minimise the opportunity for unauthorised access. The log-on procedure should, therefore, disclose the minimum amount of information about the system, in order to avoid providing an unauthorised user with unnecessary assistance. A good log-on procedure should:

- Not display system or application identifiers until the log-on procedure is successfully completed;
- Display a general notice warning that only authorised users should access the computer;
- Not provide help messages during the log-on procedure that would aid an unauthorised user;
- Validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect;

- Limit the number of unsuccessful log-on attempts allowed (three is recommended) and consider:
    - Recording unsuccessful attempts;
    - Forcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorisation;
    - Disconnecting data link connections;
- Limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on;
- Display the following information on completion of a successful log-on:
    - Date and time of the previous successful log-on;
    - Details of any unsuccessful log-on attempts since the last successful log-on.

12.8 User Identification and Authentication

All users (including ISS staff) must have a unique identifier for their personal and sole use so that activities can subsequently be traced to the responsible individual. User identifiers should not give any indication of the user's privilege level, e.g. manager, supervisor, administrator.

In exceptional circumstances, where there is a clear business benefit, or software restriction, the use of a shared user identifier for a group of users or a specific job can be used. Approval by management should be documented for such cases. Additional controls may be required to maintain accountability. The use of such group identifiers must be reviewed on a regular basis.

There are various authentication procedures that can be used to substantiate the claimed identity of a user. Passwords are a very common way to provide identification and authentication based on a secret that only the user knows. However, password methods of authentication do rely on users choosing strong passwords, changing them regularly, and not sharing them with other users. There are stronger methods of identification and authentication that should be considered to protect information classed at security level 2 or 3. Such methods include smart card or token technology and the rapidly improving biometric technology. A combination of technologies and mechanisms securely linked will result in stronger authentication.

12.9 Monitoring

The prime objective of monitoring system access and use is to detect any deviations, and to collect evidence in the event of a security incident. Such monitoring can also indicate ways and means of improving system performance and effective use of the system.

The downside of monitoring is that, if not properly managed, it can result in vast amounts of unintelligible data, and can cause performance problems (e.g. slow response times).

When choosing what to monitor, there must be a balance between collecting every possible piece of information all the time, and the effort involved in analysing the data properly once it is collected. Risk assessments to highlight the problems most likely to be encountered, or the events likely to cause most disruption, must be performed before embarking on this type of monitoring.

Many systems have their own built in monitoring software that can be tailored to the Council's requirements.

12.10 Mobile Computing and Teleworking

The risks of unauthorised access are much higher for mobile computing users and teleworkers than for those users ensconced in a, relatively, secure office environment. Mobile computers, in particular, should not hold sensitive or personal information. If the business case for holding such information on a mobile computer outweighs the security risk, then the information must be encrypted and additional security software installed on the computer. Any information held on media such as floppy disks, DVDs or CD ROMs must be stored separately from the computer equipment.

When using mobile computers, they should be so positioned to avoid unauthorised people overlooking the screen. This also applies when working with sensitive documents in a non-secure environment or public place (e.g. on a train).

All teleworkers and mobile computer users must use a strong password.

Where feasible, teleworkers must access the Council's network via a secure communications link. Those officers, Councillors and other persons given remote access who use a public telephone line link should be barred from accessing information classes at security level 2 or 3, unless adequate security measures are in place (e.g. encryption).

The controls and arrangements for teleworkers that must be considered include:

- The provision of suitable equipment and storage furniture for the teleworking activities;
- A definition of the work permitted, the hours of work, the classification of information that may be held and the

internal systems and services that the teleworkers is authorised to access;
- The provision of suitable communication equipment, including methods for securing remote access;
- Physical security;
- Rules and guidance on family and visitor access to equipment and information;
- The provision of hardware and software support and maintenance;
- The procedures for backup and business continuity;
- Audit and security monitoring;
- Revocation of authority, access rights and the return of equipment when teleworking activities cease.

12.11 Access to System Utilities

Access to system utilities must be limited to those who require such access. Where possible the following controls should be applied:

- Use of authentication procedures for system utilities;
- Segregation of the use of system utilities from applications software;
- Limitation of the use of system utilities to the minimum number of trusted authorised users;
- Authorisation for other ad hoc use of system utilities;
- Limitation of the availability of system utilities, e.g. for the duration of an authorised change;
- Logging of all use of system utilities;
- Defining and documenting of authorisation levels for system utilities;
- Removal of all unnecessary utility and system software.

13. Business Continuity

13.1 The Need for Business Continuity Planning

The Council's ability to provide its' services is at risk from a variety of disasters and security failures that may be the result of, for example, natural disasters, accidents, equipment failures and deliberate actions.

The risk of total unavailability of all the equipment (mainframe, servers, communications equipment, etc.) in the central computer room is low. Localised problems within the computer room are more common – generally caused by equipment failure.

The Council currently has no standby arrangements in case of disaster. Service Areas must note that, if a disaster destroyed the central computer room, they will be without central computing facilities for a minimum of six weeks for high priority

services. Lower priority services would be without central computer facilities for considerably longer.

The length of breaks in service for localised equipment failure, for example, a server is damaged beyond repair because of a leaking roof, will vary depending on the circumstances. To order, deliver and install a server can take six weeks. Significant delays can also occur if local office equipment becomes damaged – especially if several PC's are affected.

Paper documents are not immune from disaster type problems – fire and water can cause considerable damage.

ISS will arrange for replacement computer and communications equipment, however, it is up to the Service Areas to operate their services in the interim period. Every service area must have business continuity plans to operate their services with a minimum of disruption to the service users in the event of any (major or minor) disaster scenario.

13.2 Business Continuity Management Process

Each Service Area should have a managed process in place for developing and maintaining business continuity plans for their Area. The process should bring together the following key elements of business continuity management:

- Understanding the risks the Service Area is facing in terms of their likelihood and their impact, including an identification and prioritisation of critical business processes;
- Understanding the impact which interruptions are likely to have on the Service Area (it is important that solutions are found that will handle smaller incidents, as well as serious incidents that could threaten the viability of the Service Area), and establishing the business objectives of information processing facilities;
- Considering the purchase of suitable insurance which may form part of the business continuity process;
- Formulating and documenting a business continuity strategy consistent with agreed business objectives and priorities;
- Formulating and documenting business continuity plans in line with the agreed strategy;
- Regular testing and updating of the plans and processes put in place;
- Ensuring that the management of business continuity is incorporated in the Service Area's processes and structure. Responsibility for co-ordinating the business continuity management process should be assigned at an appropriate level within the Service Area.

13.3 Writing and Implementing Continuity Plans

Plans should be developed to maintain or restore business operations in the required time scales following interruption to, or failure of, critical business processes. The business continuity planning process should consider the following:

- Identification and agreement of all responsibilities and emergency procedures;
- Implementation of emergency procedures to allow recovery and restoration in required time scales. Particular attention needs to be given to the assessment of external dependencies and any contracts in place;
- Documentation of agreed emergency procedures and processes;
- Appropriate education of staff in the agreed emergency procedures and processes including crisis management;
- Testing and updating of the plans.

The planning process should focus on the required business objectives, e.g. restoring of specific services to customers in an acceptable amount of time. The services and resources that will enable this to occur should be considered, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities.

13.4 Business Continuity Planning Framework

A single framework of business continuity plans should be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance. Each business continuity plan should specify clearly the conditions for its' activation, as well as the individuals responsible for executing each component of the plan. When new requirements are identified, established emergency procedures, e.g. evacuation plans or any existing fallback arrangements, should be amended as appropriate.

A business continuity planning framework should consider the following:

- The conditions for activating the plans which describe the process to be followed (how to assess the situation, who is to be involved, etc.) before each plan is activated;
- Emergency procedures that describe the process to be taken following an incident which jeopardises human life and/or business operations. This should include arrangements for public relations management and for effective liaison with the emergency services;
- Fallback procedures that describe the actions to be taken to move essential business activities or support services

to alternative temporary locations, and to bring business processes back into operation within the required time scales;
- Resumption procedures that describe the actions to be taken to return to normal operations;
- A maintenance schedule that specifies how and when the plan will be tested, and the process for maintaining the plan;
- Awareness and education activities designed to create understanding of the business continuity process and ensure that the processes continue to be effective;
- The responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.

Each plan should have a specific owner. Emergency procedures, manual fall back plans and resumption plans should be within the responsibility of the owners of the appropriate business resources or processes involved.

13.5 Testing, Maintaining and Re-assessing Business Continuity Plans

Business continuity plans must be tested at regular intervals. Such tests usually highlight wrong assumptions, errors, oversights, etc. The test schedule for the plans should indicate how and when each element of the plan is to be tested. Individual components of the plans should be tested frequently. A variety of techniques should be used in order to provide assurance that the plans will operate in real life. These should include:

- Table-top testing of various scenarios (discussing business recovery arrangements using example interruptions);
- Simulations (particularly for training people in their post incident/crisis management roles);
- Technical recovery testing (ensuring information systems can be restored effectively);
- Testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site); NB Think about the effect if the removal is for a short time and a long time;
- Tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment);
- Complete rehearsals (testing that the organisation, personnel, equipment, facilities and processes can cope with interruptions).

Business continuity plans must be maintained by regular reviews to ensure that all changes are incorporated as necessary. Each plan must have a responsible officer for updating the plan, and distributing updates. Some examples of regular changes that may be required are as follows:

- Personnel;
- Addresses or telephone numbers
- Business strategy;
- Location, facilities and resources;
- Legislation;
- Contractors, suppliers and key customers;
- Processes, or new/withdrawn ones;
- Risk (operational and financial).

14. Roles and Responsibilities

14.1 Introduction

Information systems are vital to all Council activities, therefore it is appropriate that responsibility starts at the most senior level of management, but to be effective, it must be delegated to all staff.

Mangers and staff cannot avoid their own security responsibilities by placing their processing requirements in the hands of others. Service managers should clearly and formally communicate to the suppliers of computer services the level of security they require. Suppliers should then uphold the security decisions made by the service managers.

14.2 Strategic Executive Team

It is the responsibility of the Strategic Executive Team:

- To set corporate strategies for information security as appropriate;
- To inform the appropriate officers of the strategies set;
- To ensure that other corporate strategies do not conflict with the Information Security Policy.

14.3 General and Service Managers

General and Service Managers have the following responsibilities:

- Ensuring that all staff under their control adhere to the Information Security Policy;
- Allocating a suitable officer to take responsibility for all aspects of the Data Protection Act 1998.
- Setting access rules for all information under their control;
- Ensuring that computer systems are used as they were intended;

- Reporting any breaches of the Information Security Policy to Internal Audit;
- Ensuring that all staff are adequately trained in the use of information systems and their associated security procedures;
- The education of their staff on their statutory obligations;
- Allocating system administrators for all appropriate information systems under their control;
- Ensuring that appropriate business continuity plans are in place, regularly reviewed and tested:
- Ensuring that ISS are informed when staff leave the Council, or change their job.

14.4 System Administrators

For the purposes of the Information Security Policy, a system administrator is the person responsible for the day to day running and operation of an information system. System administrators are responsible for the following:

- Allocating users and privileges to information systems in accordance with the access rules defined by the appropriate General or Service Manager;
- Amending user details when an individual leaves the Council or changes duties;
- Implementing and maintaining an access register containing details of all users and their privileges;
- Securing all data on the systems under their control – including source documents where appropriate;
- Ensuring that all software under their control is properly licensed in accordance with the licence conditions of the software. This includes the retention of any licence documentation and proofs of purchase;
- Ensuring that adequate documentation exists for all systems under their control;
- Regularly reviewing all information systems under their control that store personal data. Informing the appropriate officer with responsibility for data protection of any changes required to the Council's Data Protection Notification;
- Reporting any breaches of the Information Security Policy to the appropriate manager or to Internal Audit.

14.5 Individuals

Individuals are responsible for the following:

- Changing their own passwords frequently
- Keeping their own passwords secure;
- Using strong passwords;

- Compliance with all legislation that affects their use of information;
- Only using computer systems for the purposes for which they were intended;
- Only accessing information that they are authorised to access;
- Refraining from loading unauthorised software onto the Council's computers;
- Securing their own data files on PCs;
- Refraining from using the Council's e-mail service for sending defamatory, harassing or illegal messages or attachments;
- Taking care that any e-mail is sent to the correct person;
- Reporting any breaches of the Information Security Policy to the appropriate manager or Internal Audit.
- Informing ISS if they move or dispose of any equipment or software.

14.6 Internal Audit

Internal Audit are responsible for the following:

- Advising information users on what complementary procedures to adopt to minimise the risk/temptation of fraud or misuse;
- Audit checks to ensure compliance with legislation, Standing Orders and Financial Regulations;
- Recording all incidents of any breach of the Information Security Policy;
- Monitoring staff compliance with the Information Security Policy.

14.7 Information Systems Services

Information Systems Services are responsible for the following:

- Providing appropriate software and services to assist in the security of information;
- The securing of all data and software held on the computers located in the central computer room;
- Maintaining access permissions associated with individual terminals connected to the mainframe;
- The maintenance of a list of system administrators;
- The maintenance of a software and computer hardware inventory for all purchases made by Information Systems Services;
- The provision of advice on all security matters;
- Supplying the Insurance section with an inventory of all computer hardware;
- Maintenance of the Council's data protection notification;

- Monitoring of access to the Council's network from external sources;
- Monitoring network usage to prevent unauthorised access;
- Controlling the integrity and resilience of the network;
- Ensuring that only authorised personnel have access to file servers under their control;
- Ensuring that any software written by them conforms to the Information Security Policy;
- The production, testing, and, if necessary, the implementation of disaster plans in the event of various levels of disaster befalling the Council's computer equipment;
- The maintenance of the Information Security Policy.

15. E-government and E-commerce

15.1 Publishing Information on the Internet

The Council is statutorily obliged to publish certain information. Traditional methods of publishing will be required for some time, but the Council will be publishing more and more information on its web site. The following guidelines must be considered when publishing information on the Internet:

- Do not publish personal data on the Internet (unless statutorily obliged to do so) without the informed, explicit consent of the individual. Even if the Council is statutorily obliged to publish such information, the individual must be informed;
- Protect information from unauthorised modification;
- Make sure information is regularly reviewed for accuracy;
- All web pages must have a designated owner who is responsible for the content of the page;
- General and service managers should decide on what information to publish;
- When amending content, make sure that all links point to the latest version of the page. It is often safest to delete old information rather than just remove links to it;
- Do not use copyright material on a web page.

15.2 Collecting Information via the Internet

Information collected from a visitor to the Council's website must comply with the Data Protection Act 1998. Proper security must be in place to prevent unauthorised access or tampering during the collection process and when stored.

15.3 E-transactions with a Customer

The Council does not, currently, offer anything other than a general information service on its website. In the near future this will change, and the Council's customers will be offered other

services. Where those future services include payments or sensitive information, security must be built in to those services before they become operational. Security issues to be considered are:

- *Authentication.* How do we know the customer is who s/he says s/he is?
- *Vetting.* What degree of vetting is appropriate to check payment or other information provided by the customer?
- *Liability.* Who carries the risk for any fraudulent or erroneous transactions?

When designing software or purchasing packages to perform these services, make sure appropriate security is built in, including:

- Customer or transaction details must not remain available on the input PC, Internet Service Provider server, etc. after the transaction is completed;
- Data must be encrypted before it is transmitted;
- Procedures must be in place to ensure the information arrives at the correct processing system;
- Customers, where appropriate, must be issued with a receipt for the transaction. The receipt must include a unique transaction number;
- Proper, secure audit trails must be automatically generated and maintained.

15.4 Buying via the Internet (E-procurement)

The Council does not currently order goods and/or services via the Internet. This will change in the near future. Any systems to order goods/services via the Internet must include the following safeguards:

- Goods/services to be ordered only from trusted suppliers who have proper security in place to protect the confidentiality and integrity of orders, and to prevent fraud;
- Procedures for ensuring that only authorised personnel can raise, process or input orders, authorise payment, etc. The procedures must allow for appropriate segregation of duties.
- Methods by which the supplier can authenticate that the order is genuine (e.g. digital signatures);
- Instructions for the supplier as to whom they can accept orders from, where goods can be delivered to, etc.
- Payment methods that are the most appropriate to guard against fraud;

- Agreement as to who is liable in the event of fraudulent transactions;
- Confidentiality guarantees from the supplier;
- Arrangement for encryption of transactions in transit;
- Written agreements as to what constitutes proof of dispatch and receipt of orders;
- Procedures for matching orders with deliveries and invoices;
- Contracts with the suppliers that specify security arrangements.

15.5 M-business

The use of mobile phones in business is changing. Modern phones are no longer simply a method of communicating with another phone user, they are becoming small computers in their own right. The use of these devices to access the Council's network must be subject the same type of security as a mobile computer such as a laptop.

16. Further Reading and Guidelines

The following documents can be found in *All Public Folders, Council Information, Strategy Documents, Data Protection Act 1998* folder:

- WMBC Data Protection Act 1998 – Guidelines on how to Comply.
- Information Commissioner's CCTV Code of Practice.
- Information Commissioner's Draft Code of Practice – The Use of Personal Data in Employer/Employee Relationships.

The Internet Access Policy can be found in: *All Public Folders, Council Information, Council Guidelines folder.*

The following documents can be found in *All Public Folders, Council Information, Strategy Documents, Information Security* folder:

- Security Considerations for Package Evaluation, Systems Development and Maintenance.
- PC Users Security Guide.
- Email Users Security Guide
- System Administrators Security Guide.

APPENDIX 1 – ANTI-VIRUS PROCEDURES

Precautions to be Taken Against Virus Attack

- Do not open email messages unless they are from a trusted source.
- Do not open email messages with a suspicious message header.
- Do not open any attachment within an email if you are the slightest bit suspicious.
- If you are suspicious in any way, check with the sender of the email before you open an attachment.
- If you get multiple copies of an email, or there are multiple copies in a public folder, do not open any of them without checking with the sender first.
- Update your Mcafee virus checker every two weeks from public folders or the Intranet. Whilst in this particular instance having the latest version would not have helped, there are plenty of other viruses out there which are just as (or more) destructive as the love bug. Older versions of the virus checker will not pick these up, the latest version will.
- Back up your data files (documents, spreadsheets, databases) regularly to a media other than your hard disk (server, tape streamer, floppy disk, etc.). If a virus attacks your PC, the only cure may be to wipe your hard disk clean, and rebuild your machine. This will mean total loss of all your data on your hard disk. If you have a recent, clean back up, it is a simple matter to restore your back up to your hard disk. This way, you only lose any changes made since you did your last back up.

What to do if you get a virus

The effects of a virus on your PC can be wide and varied, look for strange icons, corrupted files, odd behaviour. If you suspect you have a virus take the following action:

- Switch off your machine immediately.
- Make a note of the symptoms you spotted while they are still fresh in you memory.
- Ring the Customer Service Desk (tel.: 01922 652862).
- **DO NOT, UNDER ANY CIRCUMSTANCES,** copy or back up any of your files before you switch off – this will only result in the transfer of the virus to the media to which you copied (or backed up) the files.

APPENDIX 2 – SECURITY STANDARDS SPECIFIC TO THE VME OPERATING SYSTEM

VME is the operating system that runs the Authority's mainframe computer facility. Additional security facilities are provided to cater for the increased complexity, size and the larger number of users. These additional facilities are listed here.

NB The word "user" in this section refers to a set of software and storage space that can be accessed by authorised persons.

A2.1. **Security Levels**
(1) Except where operationally impractical, all VME users must have at least a medium security level that enforces the input of a password.

(2) Any VME user with a low security level (i.e. a security level that does not enforce a password) must have facilities limited to those required by the system. In no circumstances may a low security user have access to sensitive or personal data.

(3) All VME users that give access to privileged software must have a high security level that enforces a password and does not allow batch work to be initiated from outside the user.

A2.2. **Passwords**
(1) All MAC user password changes must be recorded to prevent re-use of the same password within an acceptable time limit.

(2) All TP systems must have a facility to change password(s) regularly.

(3) Passwords to MAC users will be changed automatically at monthly intervals if not changed by the user in the interim period.

(4) MAC users with the same password will be monitored to ensure that the same person/section/neighbourhood is not using one password for several users.

A2.3. **Live Users**
(1) Access to live users is restricted to those who require access and is limited to the period for which access is required. Requests for access to a live user are to be made to Technical Support.

(2) All MAC users produce a journal that gives details of all actions performed while a person is logged on. The facility to delete the journal when logging out (XLGT) is disabled for live users. VME will monitor and report on any access to a live user during which the journal is deleted before logging out.

(3) All journals from live users are to be retained for a suitable period by the Information Systems Services Division. Any journals removed from the

Control Section must be signed for and a log kept. The Information Systems Services Division performs spot checks on all live journals. Special attention is paid to those jobs that are not run via Helmsman (software that runs the majority of jobs in a live user).

(4) The send live procedure must be used to copy new software or versions of software to a live user. Send live journals are retained and monitored by the Information Systems Services Division.

(5) No development work is to be done in a live user.

(6) Output from systems which contain sensitive or personal data must only be given to the person designated as responsible for the output.

A2.4. **Backups**

Daily backups must be stored in a fireproof safe before the start of the next day.

Full dumps (weekly) of data and software must be stored off-site.

GLOSSARY

USER a set of software and storage space that can be accessed by unauthorised persons.

MAC Multi Access Computing. A person accessing a MAC user can issue commands and run programs.

TP Transaction Processing. A person accessing a TP system is limited to using pre-defined programs for updating or enquiring on data.

LIVE USERS. Those users that are running under a production environment, i.e. real data is used and the results of the processes are used to run the business of the Council.