Information Security Strategy

The latest version of this Strategy is available on the Council's Intranet, alternatively contact your line manager who will provide a copy.

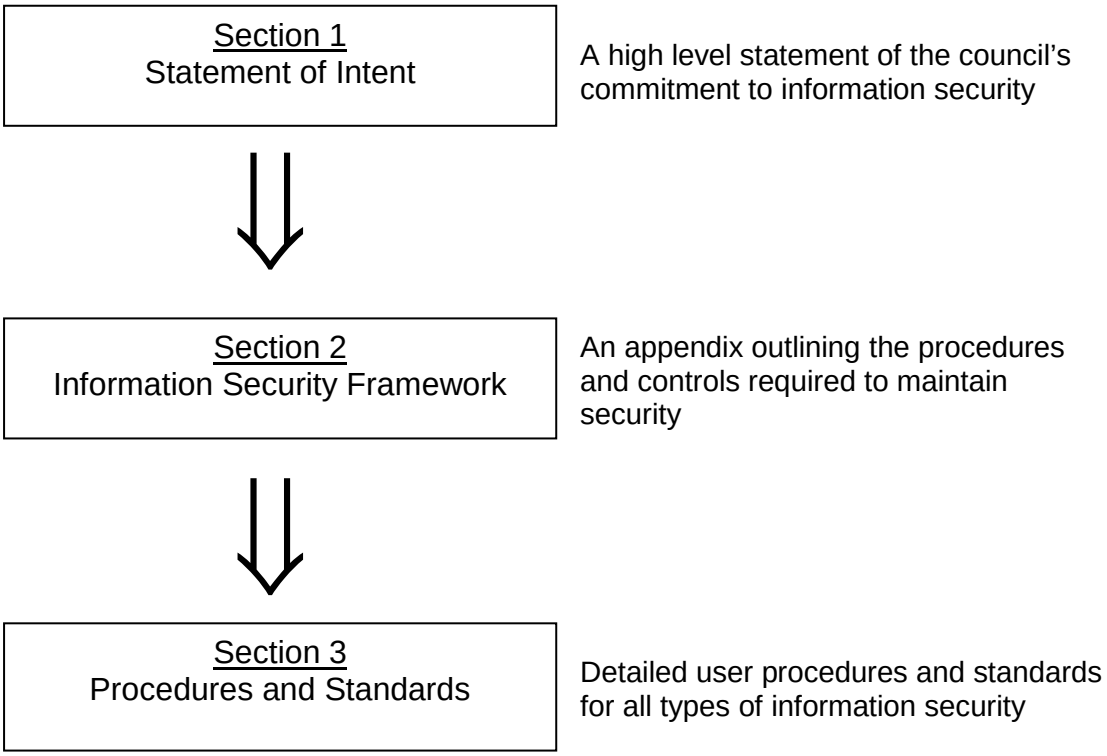
TABLE OF CONTENTS

1 Strategy Statement

1.1 Introduction

The council depends heavily on information to help provide effective services. The council also recognises that the way in which information is managed and used has significant implications in terms of service delivery, use of resources and legal compliance. The council has therefore established an Information Security Strategy based on consideration of the ISO/IEC17799:2005 standard to help protect and govern all aspects of the management and use of information resources.

The Strategy has been created utilising a three-tiered approach as outlined in the following diagram:



1.2 Objectives

The purpose of the Strategy is to: -

- Ensure business continuity
- Avoid or minimise damage by preventing security incidents and minimising their impact
- Maintain confidentiality, integrity and availability of information and information systems

The council will meet these objectives by protecting its information assets from all threats, whether internal or external, deliberate or accidental.

1.3 Statement of Intent

The council will strive to ensure that:

- Clear management direction and support for information security is provided.
- Information security is managed effectively within the organisation. See Section 2.1
- Organisational assets have the appropriate protection. See Section 2.2
- The risks of human error, theft, fraud or misuse of facilities are minimised. See Section 2.3
- Unauthorised access, damage and interference to business premises and information is minimised. See Section 2.4
- The correct and secure operation of information processing facilities is maintained. See Section 2.5
- Access to information is controlled appropriately. See Section 2.6
- Security is built into information systems. See Section 2.7
- Interruptions to business activities are counteracted and critical business processes are protected from the effects of major failures or disasters. See Section 2.8
- Breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements are avoided. See Section 2.9
- Investigative, remedial, disciplinary or legal action is taken as appropriate where policies are breached. See Section 1.6

This Statement is linked to and supported by supplementary procedures and standards that will be issued and updated as appropriate.

Authorised by.....(Chief Executive)
(Signature)

Date.....

1.4 Approach

The council will use ISO17799:2005 Code of Practice for Information Security Management, and its Corporate Risk Management Strategy as a framework to guide the approach to managing information security.

1.5 Responsibilities

It is the responsibility of each Councillor, employee and employed contractor to adhere to this and any supporting procedures and standards. Third parties not directly employed by the council but involved with council information resources are expected to comply with the law and to accept and abide by the council's information security requirements.

Where an individual has any doubt whether their intended action is allowed by the Strategy, they should check with their nominated contact (See Section 1.9) before taking the intended action.

Senior Management will demonstrate their commitment by:

- Using ISO17799 and the council's corporate risk management process as a basis for Information Security Strategy development and maintenance.
- Reviewing and approving the Information Security Strategy documentation
- Actively promoting a security culture within the council
- Disseminating the content of this strategy through the line management and democratic structures
- Using their authority to ensure there are adequate resources to implement and maintain the security strategy
- Receiving and reviewing reports on security incidents and the effectiveness of the information security strategy
- Invoking appropriate investigative, remedial, disciplinary and legal action in the event of any breach of the strategy

1.6 Enforcement

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

- Exposes the council to actual or potential monetary loss through the compromise of information or information & communications technology security
- Involves the unauthorised disclosure of confidential information or the unauthorised use of corporate data
- Involves the illegal use of data
- Disrupts any information technology system or equipment

Any breach of this strategy, actual or suspected, must in accordance with council financial regulation 23, be immediately reported to the Strategic Director, Finance and ICT who will take appropriate steps by way of investigation and report.

All security incidents must in any case be reported to the appropriate person. A log of

all such incidents will be maintained.

Breaches of the strategy may result in action under the council's disciplinary procedures, police investigation and/or legal action as the council sees fit.

Any potential activity or circumstances which for legitimate council business purposes is, or are felt to be, a justifiable exception to the requirements of this strategy, must be approved by the information security forum in writing in advance and then be logged as a security incident. Failure to gain the necessary approval before implementation may constitute a security incident and will be logged and investigated accordingly.

1.7 Supporting documentation

The following legislation should be read in conjunction with this strategy:

- Data Protection Act 1998
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Human Rights Act 1998
- Lawful Business Practice Regulations 2000
- Freedom of Information Act

1.8 Revision history

Version 1.0 – November 2005

1.9 Contact Persons

The council will ensure that each Service area has a nominated information security point of contact. Unless otherwise determined by the Service, by default this contact will be the Service's Operational Risk Co-ordinator.

Information Security Framework

2 Information Security Framework

The following security framework applies to all persons. Controls that only relate to specialist or limited numbers of employees, councillors, contractors etc will be detailed in supporting procedures and standards.

2.1 Information Security Management

To ensure that information security is managed effectively within the council a management framework will be established that will initiate and control the implementation of information security.

2.1.1 Information Security Forum

An Information Security Forum must be created and maintained. The forum will be the focal point for all information security issues within the council and will consist of representatives from:

- ICT Services – Finance and ICT
- Chief Executives Department
- Corporate Administration – Legal and Corporate Services
- Internal Audit – Finance and ICT
- Personnel Services – Human Resources

Representatives from other areas of the council and / or external expertise may be co-opted to the forum as required.

The forum will be responsible for the following activities:

- Determining and reviewing the Information Security Strategy and submitting significant changes for approval
- Monitoring significant changes in the exposure of information assets to major threats and amending the Strategy accordingly
- Reviewing and monitoring information security incidents
- Monitoring the Strategy's effectiveness

2.1.2 Authorisation Process for Information Processing Facilities

New systems or changes to existing processing facilities must be compliant with this strategy and any associated procedures and standards.

2.1.3 Security of Third Party Access

The involvement of third parties means there is not the direct control over individuals that is present in first party employment relationships. Contractual arrangements with third parties must include clauses to ensure that equal levels of security are in place.

2.1.4 Outsourcing

To maintain the security of information when the responsibility for information processing has been outsourced to another organisation, all business arrangements must be documented, must address all risks and

must include required security controls.

2.1.5 Risk Assessment

The council will select and use all reasonable, appropriate, practical and cost-effective security measures to protect important processes, assets and information systems based on a risk assessment. All risk assessments should be carried out in accordance with the council's Corporate Risk Management Policy.

2.2 Organisational Asset Classification and Control

To ensure that all information assets have appropriate security they will have an asset owner assigned and will be appropriately classified.

2.2.1 Accountability for Assets & Systems

All major assets and systems will have an identified owner. Owners can delegate responsibility but accountability will remain with the asset / system owner.

Owners will be responsible for the implementation and maintenance of security controls as well as ensuring that in conjunction with the Information Rights Officer the asset or system is compliant with the Data Protection Act and the Freedom of Information Act, especially the right of access to information.

Owners are also responsible for informing their Service Operational Risk Co-ordinators of all risks associated with their asset / system.

2.2.2 Information Classification

Assets must be classified according to the following scheme to ensure that all persons know what level of security should be applied. Asset and system owners are responsible for classifying assets and systems.

- **Personally Identifiable** - Information containing information that can be used to identify living individuals. These documents are likely to be bound by the requirements of the Data Protection Act.

- **Organisationally Sensitive** – This classification includes any information relating to activity that does not identify living individuals and may cause operational difficulties if the information became corrupted, compromised, unavailable or disclosed.

- **Public Information –** Information that does not identify individuals or include organisationally sensitive information and has not been published. This information may be subject to access requests under the Freedom of Information Act.

- **Published information** – Information which has been published, including classes of information identified in the Council's Freedom of Information Act publication scheme.

2.3 Employee Awareness

The risks of human error, theft, fraud or misuse of facilities must be

minimised. All persons handling information need to comply with this policy and any associated procedures and be aware of their responsibilities.

2.3.1 Security in Job Definition and Resourcing

All employees handling information will have their responsibilities laid out in the Employee Handbook and terms and conditions of employment.

Responsibilities include:

- Confidentiality
- Compliance with policies and procedures
- Reporting security risks and incidents

The employee's duty to keep information confidential continues even if they leave the employment of the council.

2.3.2 User Training

Services must ensure that all their employees receive appropriate information security training as part of their normal Service induction process, and that all employees processing council information receive adequate training prior to using information processing facilities or having access to information.

2.3.3 Responding to Security Risks, Incidents and Malfunctions

The information security forum will review reports on a regular basis to ensure that measures are taken to reduce the likelihood of recurrence of incidents.

Robust procedures for reporting risks, incidents and malfunctions will be defined and adhered to. All employees will be empowered to report security risks, incidents and malfunctions.

2.4 Physical and Environmental Security

Information and equipment must have appropriate levels of physical and environmental security to ensure that unauthorised access, damage and interference to business premises and information is prevented.

2.4.1 Accessible Areas

Heads of Service will ensure that accessible areas are classified based on the following criteria:

- **Open Public Area** – Areas where the public are allowed to move freely, such as corridors, waiting areas etc. Security should be based on general security arrangements, such as staff vigilance, security patrols and CCTV.

- **Controlled Area** – Areas that the public can be present in, but only following authorised access by employees / councillors (through controlled entry systems). This covers areas such as interview rooms. Once within these areas control over the public is again via employee vigilance and perhaps CCTV.

- **Restricted Area** – No member of the general public is allowed access,

except on special controlled occasions, when they are accompanied at all times by an appropriate person. Restricted areas may also be subject to further controls by limiting access to only certain employees / councillors and others when accompanied.

Within all areas there must be the appropriate levels of protection for information and information processing facilities.

2.4.2 Equipment Security

Equipment in 'Open Public' and 'Controlled' areas should have additional security controls such as 'cages' and security cables to prevent the risk of theft.

All equipment should be sited away from fire risks, explosives, water, dust, chemicals and other environmental factors that may cause damage to the equipment.

'Critical' equipment such as servers and network infrastructure should only be sited in 'Restricted' areas and have appropriately controlled environment, in terms of temperature, humidity and physical access.

2.4.3 Use of Equipment Off Site

Authorisation processes to remove equipment off-site from council premises either as a one-off or regular occurrence will be implemented. This process will take into account the following:

- Adequate insurance cover should be in place to protect equipment located off-site, and in transit.
- Equipment and media taken off premises should not be left unattended in public areas.
- Wherever possible personally identifiable and sensitive data should be removed before equipment is taken off site.
- Equipment taken off-site must have appropriate access controls applied, such as password protection

2.4.4 General Controls

The following guidance points should be included in procedures:

- Paper and computer media should be stored under lock and key when not in use, and should be disposed of appropriately when no longer required.
- Personal computers and computer terminals should not be left logged on when unattended without a council standard password-protected screensaver.
- Equipment, files, reports and other information or software should not be taken off-site without authorisation.
- Where equipment is to be reused within another location in the organisation, any data will be erased, using tools that overwrite the data.
- Equipment that is being disposed of will also be subject to erasure via overwriting before the media elements are removed and destroyed.
- Access to equipment, files, reports and other information or software should be adequately controlled and restricted to authorised persons only.

2.5 Communications and Operations Management

Communication systems and the operation of information processing facilities must be managed in a secure manner and in accordance with Council policy and procedures.

2.5.1 Operational Procedures and Responsibilities

To ensure the correct and secure operation of information processing facilities, responsibilities and procedures for the management and operation of all information processing facilities should be established. Routine duties should be documented, including:

- Operating procedures
- Change control procedures
- Incident management procedures
- Monitoring procedures

Where possible duties should be segregated to reduce the risk of accidental or deliberate system misuse. Similarly development and operational systems should be segregated to reduce the risk of accidental misuse.

2.5.2 System Planning and Acceptance

To reduce the likelihood and impact of system failure, projections of future capacity requirements should be made and where appropriate system upgrades planned.

Operational requirements of new systems should be clearly established and documented prior to their procurement and development, and tested prior to their acceptance and use.

2.5.3 Protection Against Malicious Software

To protect information processing systems and the information they hold against all forms of computer virus and other malicious software, a Gateshead Council standard that includes defensive software and employee awareness training will be developed and adhered to.

Procedures should be produced to ensure that the latest virus definitions and software engines are installed on all relevant equipment.

Additionally, employee training should include elements on malicious code awareness and preventative measures.

2.5.4 Housekeeping

Routine procedures should be established for carrying out agreed housekeeping tasks including:

- Backing-up information and systems
- Timescales for review and retention of information
- Removal and secure destruction of information

2.5.5 Network Management

Computer and communications networks should be managed appropriately to ensure that information is protected.

2.5.6 Media Handling and Security

To prevent damage to assets and interruptions to business activities, media should be controlled and physically protected.

Appropriate procedures will be established to protect paper documents and computer media from damage, theft, unauthorised access and misappropriation.

2.5.7 Exchanges of Information and Software

Guidelines and protocols should be adopted to ensure the following:

- Information is protected from unauthorised disclosure, modification and loss during the exchange process
- The exchange is compliant with relevant legislation and regulations

2.6 Access Control

Access to information assets should be controlled on the basis of business and security requirements and the user's role in the council.

2.6.1 Business Requirements for Access Control

Access to systems and information must be on a need to know and need to use basis.

2.6.2 User Access Management

Formal procedures should be in place to control the allocation of access rights to information systems and services. These access rights should be reviewed on a regular basis and revised as necessary.

2.6.3 User Responsibilities

Users must be made aware of their responsibilities for maintaining effective information access controls, particularly with regard to the use of passwords.

2.6.4 Network Access Control

Access to networks and any networked services should be controlled to ensure that only authorised users have access.

2.6.5 Operating System Access Control

Security facilities at the operating system level should be used to restrict access to computer resources that may undermine security, in particular terminal identification, system time, system logs and authentication mechanisms.

2.6.6 Application Access Control

To prevent unauthorised access and enable accountability, information processing facilities applications should have access control mechanisms.

2.6.7 Monitoring System Access and Use

System owners will develop procedures for monitoring systems to ensure system security, compliance with policies and procedures and provide evidence in the event of a security incident or investigation. All monitoring

will be compliant with legislation and in particular the Lawful Business Practice Regulations 2000 and the Regulation of Investigatory Powers Act 2000.

Monitoring will include checks for failed access attempts, data manipulation, spot-checks and any other logged system event as appropriate.

Only authorised and trained staff will conduct monitoring.

Users will be informed of monitoring activity during training on each system.

2.6.8 Mobile Computing and Teleworking

All equipment, software and procedures used when employees are working in a mobile computing and teleworking situation must have security measures in place to maintain the levels of information security otherwise required by the Strategy when not working in a mobile computing and teleworking context.

2.7 System Development and Maintenance

To ensure that information security controls are built into information systems, security requirements will be specified at the design stage. Additionally, changes and maintenance to existing systems will ensure that security is maintained.

2.7.1 Security Requirements of Systems

To ensure that information governance controls are built into information systems and information processes, governance requirements will be specified prior to, and implemented in, development projects. Existing governance elements will be regularly reviewed.

2.7.2 Security in Application Systems

All application systems used for council business purposes must include security measures appropriate for the information they process.

2.7.3 Cryptographic Controls

Cryptographic controls will be applied to information resources where the level of risk deems this to be appropriate.

2.7.4 Security of System Files

Security of system files will be applied to information resources where the level of risk deems this to be appropriate.

2.8 Business Continuity and Management

To counteract interruptions to business activities and to protect critical council processes from the effects of major failures or disasters, the council will develop a process for the management of business continuity. To ensure a consistent approach is adopted, it must comprise of:

- Risk assessment and management procedures
- Plan management, development and testing responsibilities guidelines
- Documentation guidelines

2.9 Compliance

The Strategy aims to ensure there are no breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

2.9.1 Compliance with Legal Requirements

Council wide policies covering specific legislation such as the Data Protection Act will be adopted.

To ensure that each system is compliant with relevant legal, statutory, regulatory or contractual obligations the system specific policy must list all applicable requirements and detail how they are being met.

2.9.2 Reviews of Security Strategy and Technical Compliance

To ensure compliance with the current requirements procedures and standards must be reviewed on a regular basis and where appropriate up dated.

2.9.3 Audit Considerations

Any information system procured or developed for council business use must be auditable by providing for audit use, read-only access to all parts of the system, full information retrieval facilities and detailed audit trails and logs.

Audit of adherence to the Information Security Strategy and its supporting procedures and standards will be carried out by the councils Internal Audit Service as part of its regular planned audit work and as authorised by the council's constitution and appropriate legislation.

Breaches of the strategy and its supporting procedures and standards will be investigated as considered appropriate by Internal Audit.