Information Security Strategy

Document Owner: Chief Information Officer
Version: 1.1
Date: May 2011

We will on request produce this Strategy, or particular parts of it, in other languages and formats, in order that everyone can use and comment upon its content.
1. **INTRODUCTION**

1.1 **Purpose**

Information is the single most important asset for any public sector body. This Strategy lays down the principles by which Suffolk County Council will protect the information under its control.

1.2 **Definition of Information Security**

Information security is the practice of ensuring information is only read, heard, changed, broadcast and otherwise used by people who have the right to do so. It requires a range of skills and knowledge and increases in importance as use of and reliance upon information grows.

1.3 **Background**

1.3.1 This Strategy is required by and forms part of the overarching Corporate Information Management and Data Security Strategy.

1.3.2 The Strategy has been developed with reference to best practice guidelines contained within ISO/IEC 27001\(^1\) and ISO/IEC 27002.\(^2\)

1.3.3 There are also a number of good business reasons for the development and adoption of an Information Security Strategy and associated corporate policies:

- **Dependency on Information Systems**
  Over recent years there has been a significant increase in reliance on information systems to hold and process information that is critical to Council business. Much of this information contains sensitive and confidential details, which our citizens and customers entrust to us and which would cause serious damage to the organisation if a breach of confidentiality or loss of data occurred.

- **Dependency on Manual Records**
  Despite the rapid increase in electronic data the Council holds and remains dependent upon manual records for the discharge of effective and efficient service delivery. Furthermore, the Council is bound by legislation (e.g. Local Government Act 1972) to make ‘proper arrangements’ for the records it creates, to ensure their availability and accessibility to the public, and to provide for their retention, as required. As with electronic data, all such arrangements must provide for appropriate security and the mitigation of risks associated with manual records being lost or compromised.

- **Degree of Information Sharing**
  As the Council moves forward to meet the objectives of its New Strategic Direction

---

\(^1\) ISO/IEC 27001 Information Security Management System (ISMS).

(NSD), divestment and shared services will be required. This will necessarily involve the increased sharing of information, with partners, other organisations and agencies. It is imperative that the controls and processes are in place not only to ensure that data is properly protected, but also to ensure that the Council continues to meet its obligations under legislation, particularly the Data Protection Act 1998.3

- **Challenges of Controlling Information**
  There is a vital requirement to ensure that the control environment of information is appropriate to the information classification. There should be arrangements in place to ensure that information deemed to have a level of sensitivity requiring safeguards above the norm is not subject to unnecessary or avoidable risk as provided for and detailed in the Council’s Protective Marking Policy.

- **Laws Relating to Information Security**
  In addition to being good business practice, there are a number of laws and regulations that affect information security practices. Particularly relevant are the requirements to comply with the Data Protection Act 1998, the Computer Misuse Act 1990, the Copyright, Designs and Patents Act 1988 and the Human Rights Act 1998 but other requirements are gaining increased importance, e.g. Privacy and Electronic Communications (EC Directive) Regulations 2003.

- **Increasing Use of Remote Access**
  With changes in technology, the use of remote, flexible and mobile working is becoming increasingly commonplace. Any accommodation review will also require much more flexibility in the way the Council works and, therefore, the risk of exposure to an information security incident is increased.

1.3.4 **Internationally Recognised Standards** - The internationally recognised standards for information security are published as:
- ISO/IEC 27001 Information Security Management Systems - Requirements;

These standards set out the requirements to protect:
- **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.

1.3.5 **The Benefits of Information Security** - There are a number of benefits in introducing and adopting this Information Security Strategy and associated policies:

---

Data Protection Act 1998 Schedule 1 Section 7: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
♦ **Requirement of the Market** - As the Council moves forward with the NSD, there will be enhanced and expanding opportunities to work with other authorities, partners and organisations. This will require the Council to have appropriate technical and organisational security measures in place to ensure and provide for secure, trusted and efficient information sharing and data exchange.

♦ **Prevention Better Than Cure** - For residents, businesses, organisations and others within Suffolk (and beyond) to have confidence in the fact that information provided to the Council is safe and secure, it is essential that the appropriate assurance framework is in place. The financial and reputational risks surrounding the loss of vital data must not be underestimated, nor the time and costs that would be required in responding to any incident.  

♦ **Senior Management Requirement** - That arrangements are in place and monitored to ensure that incidents are minimised, if not eradicated, and appropriate action (including action under the Council’s disciplinary process) taken should any incident occur.

### 1.4 Scope

This Strategy applies to all staff, councillors, volunteers, partners and third-parties handling the Council’s data and information.

### 1.5 Aims and Objectives

The Council’s aims and objectives with respect to information security management are to:
- embed information security management into the culture of the Council;
- develop a framework of information security policies; and
- provide assurance to all stakeholders that the Council has appropriate information security arrangements in place.

### 1.6 Linked Protocols/Policies/Procedures

This Strategy should be read in conjunction with the following corporate policies, strategies, protocols, procedures and standards:
- Acceptable Use of ICT Policy
- Clear Desk Policy
- Corporate Information Management and Data Security Strategy
- Data Protection Policy
- Data Quality Policy
- E-Mail Acceptable Use Policy
- Freedom of Information and Records Management Policy
- ICT Remote Working Policy
- Information Security Incident Management Policy

---

4 In 2009, the cost to UK organisations for each individual electronic record per data loss was calculated at £64 (source: Pretty Good Privacy - [http://www.pgp.com](http://www.pgp.com)).
1.7 Roles and Responsibilities

These are set out in the Suffolk County Council Information Security Policy, and in the Corporate Information Management and Data Security Strategy.

2. STRATEGY

The Council’s Information Security Strategy is formed out of the following linked themes and activities:

- a clear statement from senior management;
- the development of an appropriate ICT and related infrastructure;
- a set of policies and procedures;
- ensuring staff and others (listed in Section 1.4) are properly informed and behave accordingly;
- the establishment of appropriate governance structures;
- appropriate assurance;
- engagement with partner organisations on the above where appropriate; and
- an action plan to deliver the above.

2.1 Code of Connection and Non-Disclosure Agreement

2.1.1 The Council has recognised that there is a need to share in a secure manner information between partners, and with other central Government secure networks such as GCSX (Government to Government), CJIT (Criminal Justice), N3 (NHS), PSI (Police), as well the need to comply with standards such as the Payment Card Industry Data Security Standard (PCI DSS) devised by the PCI Council.

2.1.2 To enable third-party organisations to connect to Council networks, appropriate security controls need to be in place and Code of Connection and Non-Disclosure Agreement documentation must be completed.

2.1.3 The Code of Connection and Non-Disclosure Agreement set out the minimum information security requirements for compliance with industry standards, or for connection to the Council network, which must be achieved and maintained by the third-party organisation wishing to connect. It commits that organisation and its employees to compliance with the requirements of the Code. Accordingly, it
must be signed by an individual from the organisation who carries the specific authority of the Director, plus a nominated individual responsible for security. Until these documents are completed, with the required sign-offs, then access to the Council network will not be granted.

### 2.2 Information Sharing Framework

(Further details are available from [http://www.transformingsuffolk.co.uk/](http://www.transformingsuffolk.co.uk/))

In addition to the Suffolk Strategic Partnership Information Sharing Protocol, outlined above, the Council will work with other organisations to develop information sharing protocols such as the Suffolk Children’s Trust Partnership Information Sharing Charter as well as establishing service-specific data exchange agreements (DEAs) with those partners with whom information is shared on a regular basis.

### 2.3 Data Transfers

Please refer to the document: Technical Measures for Securing Bulk Data Transfer to and from Third-Parties.
2.4 Framework for Information Security

The above reflects the Council’s position as at 31 January 2011.
3. **DELIVERING THE STRATEGY**

3.1 **Information Security Management System (ISMS)**

3.1.1. The Strategy to deliver the information security arrangements is based on current best practice and is in line with recognised standards as described earlier.

3.1.2 The Plan, Do, Check, Act Model (below) demonstrates the quality framework for both the introduction and implementation of an Information Security Management System.

3.2 **The Plan, Do, Check, Act Model**

This process involves the following activities:

3.2.1 **ISMS Programme Management** - There are three main aspects to the ISMS programme:

- the awareness throughout the organisation of roles and responsibilities regarding information security;
- the development and adoption of the information security management system; and
- the on-going monitoring and management of information security including responding to changes in legislation and practice, and managing and reporting security incidents.

3.2.2 **Determining the ISMS Strategy** - The Corporate Information Management and Data Security Group to identify, based on risk analysis methodology, the critical service areas where security incidents would have the highest potential impact in terms of information loss, reputation and on-going service delivery by:
undertaking a review of current business processes to identify critical information in terms of value to the organisation;

applying the risk management methodology to ascertain the appropriate classification and handling schemes that should apply;

developing an information asset register to ensure that appropriate information, and those responsible for such information are identified; and

ensuring that the appropriate control arrangements are in place to minimise the risk of information security incidents occurring.

3.2.3 Developing and Implementing an ISMS Response - Information security incidents should be identified, responded to, recovered from and followed-up using information security management and reporting processes:

- All employees, contractors and third-party users must be made aware, by relevant managers, of their responsibilities to report any information security incidents as quickly as possible, as well as being aware of what procedures to follow.

- Identification of information security incidents, including the completion of information security incident reports, assessment of business impact, categorisation and classification of the incidents, are the responsibility of the relevant manager.

- Subject to the circumstances responsibility for responding to information security incidents, including their investigation, containment, and the eradication and cause of the incident will be led by the Head of Corporate Information and Records and/or CSD Policy and Compliance Manager.

- The same officers, jointly or separately, to ensure recovery from the incident, including rebuilding systems and restoring data, and the closure and management reporting of the incident.

3.2.4 Exercising, Maintaining and Reviewing - The Corporate Information Management and Data Security Group to ensure that the Information Security Strategy and associated policy and procedures are fit for purpose and kept up-to-date. A programmed series of reviews will enable the Council to:

- demonstrate the extent to which the Strategy and policies are complete, current and accurate;

- ensure that changes in associated legislation and business practices are incorporated into the framework; and

- provide an opportunity for the wider organisation and appropriate partners to input into the information security framework.

3.2.5 Maintaining and Auditing the ISMS - In order for information security to be successfully incorporated within the Council it must be regarded as an integral part of the normal management process. To ensure that the ISMS continues to provide an effective assurance framework for the Council it will be monitored regularly and appropriate results reported to, the Chief Information Officer, Senior Information Risk Owner and the Corporate Information Management and Data Security Group. These monitoring reports will encompass:

- the effectiveness and efficiency of information security arrangements;

- the identification of areas where improvement is required;
information and systems subject to unacceptable levels of risk; performance against quantitative, objective targets; and actions required to minimise or eradicate risk.

In addition to the monitoring reports, the Corporate Information Management and Data Security Group will ensure the maintenance of all aspects of information risks including:
- criticality of information;
- identified vulnerabilities;
- level of threats;
- potential business impacts; and
- status of security controls.

FURTHER ADVICE

For day-to-day practical advice and guidance on this Strategy, please contact:

Suffolk County Council Information Management Services
01473 264618
information.management@suffolk.gov.uk

CSD Policy & Compliance Team (via the CSD IT Helpdesk)
01473 265555
ITHelpdesk@csduk.com

GOVERNANCE

This Strategy is sponsored by:
- Director of Resource Management (Senior Information Risk Owner).

Responsibility for maintaining and updating this Strategy belongs to:
- Chief Information Officer.
### DOCUMENT CONTROL

#### Changes History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Amended By</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.a</td>
<td>December 2010</td>
<td>Neal Scarff</td>
<td>Draft</td>
</tr>
<tr>
<td>0.b</td>
<td>January 2011</td>
<td>Stephen Carr, Tim Wetten &amp; Neal Scarff</td>
<td>Amendments</td>
</tr>
<tr>
<td>0.c</td>
<td>January 2011</td>
<td>Doug Reed, Stephen Carr &amp; Neal Scarff</td>
<td>Amendments and Additions</td>
</tr>
<tr>
<td>0.d</td>
<td>February 2011</td>
<td>Doug Reed</td>
<td>Minor Amendments</td>
</tr>
<tr>
<td>0.e</td>
<td>February 2011</td>
<td>Tim Wetten</td>
<td>Amendments</td>
</tr>
<tr>
<td>0.f</td>
<td>March 2011</td>
<td>Doug Reed</td>
<td>Amendments</td>
</tr>
<tr>
<td>0.g</td>
<td>March 2011</td>
<td>Tim Wetten</td>
<td>Amendments</td>
</tr>
<tr>
<td>1.0</td>
<td>April 2011</td>
<td>Doug Reed</td>
<td>Various changes based upon feedback via Strategic Information Agents</td>
</tr>
<tr>
<td>1.1</td>
<td>May 2011</td>
<td>Doug Reed</td>
<td>To reflect approval (subject to one minor textual change) by the Corporate Information Management and Data Security Group</td>
</tr>
</tbody>
</table>

#### Approval (SCC)

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Signed</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>