

London Borough of Sutton**Audit Committee - 16th April 2009****Report of the Head of IT****INFORMATION MANAGEMENT SECURITY UPDATE****Ward Location:** Not Applicable**Author(s) and Contact Phone Number(s):**

Nick O'Reilly

Area Served: Borough Wide**Executive Councillor: Colin Hall****Summary**

This report summarises progress implementing enhanced information management security arrangements and with achieving the requirements of the Government Connect secure intranet connection.

Recommendations

I recommend the Committee to:

- 1) note the progress made in respect of enhancing information security outlined in this report

1. Background

The Audit committee received a report on information security in September 2008; it was agreed to provide an updated report in April 2009.

Since September 2008 the main focus has been on achieving the code of connection requirements without which we would not be allowed to access Department of Work and Pensions Data required to process benefits.

2. Progress Made

We submitted our first government connect compliance statement in December 2008; following which we had four further iterations before the government assessor passed our submission as compliant. This is typical of the experience of most Councils who have also had to make multiple submissions. We received approval on 23rd March; and our connection is due to be implemented on 9th April.

As part of the government connect process we have replaced and upgraded 14 firewalls to provide enhanced security for the council's network; introduced secure complex passwords for all users and improved the secure physical segregation of public access, schools access and staff access where we have all three in use.

We have purchased and tested new on line training for all users covering 3 aspects of information security:

- Data Protection
- Information Security
- Freedom of Information

This was delayed to allow us to purchase a single corporate tool for all on line training including staff induction, health and safety and other policy based training. The tool we have bought is used by over 100 councils and as part of this we have access to courses published by others that we can amend and adopt locally. This is due to be launched for all users during April; Revenues and Benefits staff needing to access DWP data have piloted the courses.

We have reviewed existing Information Security polices and as a result we are taking a number of steps to make these easier to understand and use:

- A series of one side A4 briefings published on the intranet (4 to date) (see example in Appendix 1)
- Two Insight articles and two Intranet front page bulletins have been issued
- Introducing a new :
 - one page information security statement (see Appendix 2)
 - 5 page information security policy (replacing a 28 page document)
 - A new monitoring policy that explains how we monitor user activity
- Reviewing with a view to adopting a new series of 15 information security polices developed by the West Midlands LGA and endorsed by the Department of work and Pensions. (It is hoped these become standard policies for Councils throughout the country).

The ICT code of conduct was approved and letters issued to all staff and all contractors. Over 65% of staff have signed the revised ICT code of conduct; we did allow 12 months to complete this task and both Chief Executive's and Resources service groups now have all staff signed. In April all staff yet to sign and return acknowledgement of the ICT code of conduct will receive a reminder letter.

3. Issues Arising and/or Outstanding

Since September there have been seven reported information security incidents:

- A laptop stolen from the boot of an employees car (the employee had packed the laptop ready for a journey to work)
- Some confidential materials dumped in a skip at the civic centre and not using the confidential waste procedures (these were retrieved and disposed off correctly)
- A laptop used by the hospital tuition service stolen from hospital premises
- A laptop used by an emergency duty team social worker stolen from their home
- A memory stick used by a social care worker stolen from their home
- A break in and theft of 8 computers from the drapers centre offices
- 4 laptops and one mobile phone stolen from the Behavioural Support Team at the Sutton West Centre

The fact that these have all been reported using the agreed procedure, and incident reports completed shows there is a better understanding of our information security processes. In each case an impact assessment was undertaken, having quantified the amount of personal data involved in four cases we have reported the incident to the Information Commissioners Office, in two cases we have notified customers affected. The last case is still under investigation. However in each case we believe the risk of the data being compromised is low.

The main outstanding action is to provide encryption tools for staff that have

laptops; and/or need to copy data to portable media. We are in the final stages of completing a tender and evaluation of the preferred product; which will then be rolled out to users.

The proposed information audit and classification toolkit was developed; and has undergone a number of pilots. However the feedback has been this is difficult to use, not made easier by the lack of an agreed standard definition or risks and category levels for local government. The national impact levels apply mainly to central government. It has been suggested that a national definition will shortly be agreed. This work was also a casualty of the considerable workload involved with the government connect submission, which had to be prioritised due to the absolute deadline imposed by the DWP.

4. Financial Implications

None directly from this report, see financial implications in the report to Executive (Appendix B)

5. Influence of the Council's Core Values

The way the Council collects processes and maintains the information it holds about both citizens and businesses is fundamentally important to build trust, confidence and respect with the community.

The need for robust data sharing arrangements with partners that include security arrangements is also essential in building services for the community that are delivered in partnership.

6. Equality Impact Assessment

None directly from this report.

7. Background Papers

Report to Audit Committee 18th September 2008

**Appendix 1 – Example 1 Page Briefings****Purpose**

Users Passwords are an important component of information and network security. The password serves to identify and authenticate a user to systems resources and information assets.

It is through the use of authentication access that London Borough of Sutton can be assured that its information and systems are being accessed by authorised system users. It is therefore essential that adequate measures are taken to create secure passwords and to safeguard them in accordance with the guidelines below.

Responsibility

Authorised System Users are responsible for the creation of secure **passwords** and for keeping them safe.

Guidelines

This document contains guidelines on how to create; change and safe guard your passwords.

Changing passwords

- Passwords changes will be enforced by the system 45 days after creation. Users will be notified on login one week in advance of password expiry. At that point and at every subsequent login until a change is made, users will be prompted to select a new password.
- When changing your password do not use one that you have used to access the system before. To safe guard against this the system keeps a record, up to 24, of the past passwords you have used and will not allow you to reuse them.

Safe guarding Passwords

- Your password must only be known by you and never disclosed to another, no matter who they are.
- Your password should be changed immediately if you suspect someone has had access to your password
- Passwords should never be written down, especially in locations where other may gain access to them.

Creating a Secure Password

- Passwords must be at least 8 characters long.
- Passwords should comprise 3 different character sets:-
 - upper case letters
 - lower case letters
 - Numbers
 - Other keyboard characters
- Passwords should not be based on any wording or number combination that can be associated with the password owner e.g. postcode, car registration, family member's name.

Where can I find the 'Password Policy?'

- The Policy on password usage is included within the ICT code of conduct.
- The ICT code of conduct is available alongside all information security policies and can be found on the Intranet in the corporate section under information security.

PLEASE NOTE: When referring to any of the Information Systems Policies, Procedures or Guidelines please check you have the latest's version as published on the Intranet



Obligation to our Customers

We have a duty to our customers to protect the confidentiality and integrity of the data we hold about them.

This obligation is both statutory (from the Data Protection Act) and governed by the Information Commissioners Office codes of practice.

Our Customers have the right to know how we protect their data, and if they believe its security has been breached can complain to the Information Commissioner.

The Information Commissioner has the power to investigate such complaints and can levy fines on individuals and on the Council as an organisation.

Storing Data – Minimising Risks

- Whenever Possible Store data on the network server and not on your computer desktop, local drive or portable media. That way it is both backed up and is not at risk if your computer is stolen.
- If you have to copy files to your local computer or to portable media then consider is the data confidential or sensitive. If it is you should at least password protect such files; and you may need to use encryption tools to secure such data (see later).
- If you need to copy files to portable media to carry out you job, then as soon as possible copy the amended files back to the network, and delete them from the portable media.

Portable Media covers memory sticks, cd's, dvd's, flash drives and such like.

Laptops and Other Portable Devices

- If you have a laptop, blackberry, palmtop or portable media at home or in the office, if possible lock it away overnight and/or when you are not present. If it cannot be locked away at least store it out of sight.
- Never leave your laptop, blackberry or other portable device un-attended in your car; always carry laptops in the boot.
- Take care when carrying such devices in public places, do not use them unless absolutely necessary.

Basic Data Security at Work

- Always lock your computer when you leave your desk even for a short period.
- Check you have a password protected screensaver that is set to activate after 15 minutes of inactivity.
- Always log out of your computer when you leave your desk for more than 15 minutes.

Encryption

- From April 2009 Encryption tools will be available to users who need to store confidential data on laptops or on portable media.
- Encryption works by scrambling data content and only allowing users with the encryption password or token to decode the information.
- You should still store data on the network whenever possible as encrypted data is not backed up.

PLEASE NOTE: When referring to any of the Information Systems Policies, Procedures or Guidelines please check you have the latest's version as published on the Intranet



Appendix 2 – New Information Security Statement (due for ratification by CMT 15th April)

Information Security Statement

The objective of this statement is to provide executive direction for the protection of information owned by the London Borough of Sutton and our citizens, partners or suppliers in whatever form it may be held or communicated, whether verbal, on paper or electronic. Information is one of our most valuable assets. Of equal value is the trust of our partners and clients that we will protect the information that they have shared with us.

LBS proprietary and client, partner or supplier information, when created, stored, transmitted or communicated, must be protected from unauthorised access, use, modification or destruction. Consequently, all access to, and use of this information and data, requires adherence to the following policy principles:

- **Confidentiality** - Appropriate measures must be taken to ensure that LBS proprietary, private, or client information is accessible only to those authorised to have access.
- **Integrity** - The accuracy and completeness of LBS information must be maintained and all changes or modifications affecting that information must be authorised, controlled, and validated.
- **Availability** – Information must be available to authorised individuals when required. In the event of a disaster or malicious attack, the Council's information and the systems critical to the ongoing activities of the Council must be recoverable.
- **Authentication** - All persons and systems seeking access to information, or to our networked computer resources must first establish their identity to the satisfaction of the Council.
- **Access Control** - The privilege to view, or modify information, computer programs, or the systems on which the information resides, must be restricted to only those whose job functions absolutely require it.
- **Auditing** - User access and activity on each of the Council's computers, firewalls and networks must be recorded and maintained in compliance with all security, retention, legislation and regulatory requirements.

Security policies are in place to support these objectives, together with detailed procedures.

The Head of I.T. has responsibility for maintenance of the Security Policies, which will be reviewed annually by the LBS Information Security Management Board.

All managers are responsible for implementing the Security Policies within their areas, and for adherence thereof by their staff.

It is the responsibility of each member of staff to adhere to LBS Security Policies.

This statement has been approved by the Chief Executive.

Chief Executive

Date