# AUDIT COMMITTEE

## *Committee Report*

**Public**

**Date of Meeting:** **4th December 2009**

**Title:** **ICT Security Policy and Annexes**

**Report of:** **Head of Audit Services**

**Report reference:** **CORP 53/09**

**Summary:**
This report apprises Members of progress to date on the recommendations contained in the Audit Report relating to the Council's ICT security Policy and Annexes

**Recommendations:**
Members are requested to receive this report.

**Contact Officer:** Ian Beckett, Head of Audit Services **Ext:** 7292

Chairman and Members of the
Audit Committee

4th December 2009
CORP53/09

# Audit of ICT Security Policy and Annexes

## 1 Background

1.1 The Audit Services' report relating to the review of the Council's ICT Security Policy and Annexes was presented to Members of the Audit Committee at the meeting held on 22nd June 2009 – Report CORP 20/09 (Appendix B) refers.

1.2 At the meeting of the Audit Committee held on 25th September, the Audit Commission's Audit Manager reminded Members that this report had been issued, and drew attention to the recommendations made therein. He emphasised the Audit Committee's role in progressing and monitoring the matter. (Minute AUC 51/09 refers).

1.3 The Committee resolved that the Head of Audit Services be requested to submit a report outlining progress in addressing the issues identified. It was further agreed that a special meeting of the Committee would be convened to deal with the matter should that be deemed necessary.

## 2 Current Position.

2.1 A schedule has been received from the Infrastructure and Network Manager that gives the position in relation to each of the recommendations. This is attached as **Appendix A** to this report for Members' information.

## 3 Recommendation

3.1 Members are requested to receive this report.

I. Beckett
Head of Audit Services
December 2009

# APPENDIX A

**Summary of Actions**

| Grade | Not Started | In Progress | Completed | Total |
|---|---|---|---|---|
| A | | | 2 | 2 |
| B | 2 | 1 | 10 | 13 |
| C | 5 | 2 | 20 | 27 |
| D | | | 4 | 4 |
| N/A | | | 2 | 2 |
| | 7 | 3 | 38 | 48 |

**Notes:**

Of the seven tasks not started none are the responsibility of the Head of ICT.
Of the three tasks that are currently in progress, two are to be implemented once the ICT shared service with Allerdale BC takes place.

| ***Ref*** | ***Responsible Officer*** | ***Recommendation / Agreed Actions*** | ***Grade*** | ***Suggested Timescale for Completion*** | ***Status as at 15/09/2009*** | ***Tasks*** |
|---|---|---|---|---|---|---|
| A.1 | Head of ICT | The new strategy should be agreed and released to replace the expired one as soon as possible. This will almost certainly require collaboration with Allerdale to satisfy the requirements of ICT Shared Services.<br><br>*Since the audit, a new Shared IT Strategy has been produced. The strategy has been already been approved by Allerdale and goes before Carlisle City Council's Executive on the 5th May.* | B | November 2009 | Completed | |
| A.2 | Head of ICT | Given the impact to IT users, it would be good practice to ensure that future IT strategies are published to the employee intranet.<br><br>*The latest IT strategy will be published on the intranet once it has been approved.* | C | November 2009 | Completed | |
| A.3 | Head of ICT | An implementation timetable should be drawn up to ensure all security principles are adopted and enforced as soon as possible. | B | November 2009 | Completed | A timetable has be produced as part of the CoCo compliance this will be implemented. |
| A.4 | Head of ICT | The group should review its future purpose and structure and decide whether the concept of bi-monthly meetings is a realistic prospect in the light of the Allerdale Shared Service arrangements. | C | November 2009 | Completed | An ISG was held on 23rd September to discuss this. The ISG has now been dispanded. |
| A.5 | Head of ICT | As per the ICT Security Policy principles, written standards, instructions and working methods should be drawn up for the following areas:-<br><br>❑ Acquisition procedures<br>❑ Documentation and recording<br>❑ File and data control<br>❑ Security and safety<br>❑ Communications<br>❑ Processing and handling of data<br>❑ Housekeeping | B | November 2009 | Active | **This will be implemented as part of the Shared ICT service.**<br><br>A number of these standards have already been started |

| Ref | Responsible Officer | Recommendation / Agreed Actions | Grade | Suggested Timescale for Completion | Status as at 15/09/2009 | Tasks |
|---|---|---|---|---|---|---|
| | | See also recommendation A8.<br><br>*The audit exit meeting established that as part of the Shared Service Strategy with Allerdale, the ICT Section would be implementing ITIL principles. The introduction of the areas highlighted above would be a part of this.*<br><br>*N.B. ITIL is the Information Technology Infrastructure Library and is a set of concepts and policies for managing Information Technology infrastructure, development and operations. In other words, a best practice approach.* | | | | |
| A.6 | Head of ICT | It would be good practice to implement adequate procedures to monitor current capacity and periodically calculate future capacity requirements.<br><br>*The audit exit meeting established that disk capacity V's usage is monitored monthly along with the Exchange email server. However, capacity planning is part of ITIL and therefore improvements will probably be identified.* | C | November 2009 | Active | **This will be implemented as part of the Shared ICT service.** |
| A.7 | Head of ICT | A database of information security threats and remedies should be created and maintained. | C | November 2009 | Completed | IT Services uses Microsoft and other software vendors' knowledge bases to monitor security threats, along with our virus software vendors threat database. |

| Ref | Responsible Officer | Recommendation / Agreed Actions | Grade | Suggested Timescale for Completion | Status as at 15/09/2009 | Tasks |
|---|---|---|---|---|---|---|
| A.8 | Head of ICT | Standards and procedures should be established for the following areas:-<br><br>❑ The information security policy<br>❑ The file management policy<br>❑ The access control policy<br>❑ The password management policy<br>❑ The system, file and data back-up policy<br>❑ The file and data retention policy | B | November 2009 | Completed | This forms part of the timetable produced as a consequence of ref. A.3. This will be completed as per the timetable.<br><br>**Anticipated completion date: 27st November 2009.** |
| A.9 | Head of ICT | Guidance notes should be established for laptop users. These could also be uploaded to the employee intranet for future reference. | C | November 2009 | Completed | This forms part of the timetable produced as a consequence of ref. A.3. This will be completed as per the timetable.<br><br>**Anticipated completion date: 27th November 2009.** |
| A.10 | Head of ICT | Password management should be enforced through Windows group policy as a basic security requirement as soon as possible e.g. changing of passwords over a set time interval and strong passwords<br><br>❑ A minimum of 6 characters in length<br>❑ A mixture of symbols, numbers and letters<br><br>*It was agreed in the audit exit meeting that this was a fundamental weakness of the Authority's IT infrastructure. It will be resolved once the Microsoft Office and Windows XP rollout has been completed. It was established that a 6-month timescale for implementation of this recommendation is a reasonable expectation.* | A | November 2009 | Completed | This will be implemented by the **16th October 2009**. |
| A.11 | Head of ICT | Management should assess the value of having a media record of non-Microsoft software covering the | D | November 2009 | Completed | This will be introduced as part of an update to our asset |

| Ref | Responsible Officer | Recommendation / Agreed Actions | Grade | Suggested Timescale for Completion | Status as at 15/09/2009 | Tasks |
|---|---|---|---|---|---|---|
| | | following:-<br><br>❑ The date of purchase and installation<br>❑ The software version number<br>❑ The vendor's name and contact details<br>❑ Related release and/or patch details (dates, references, etc)<br>❑ The location of the software, both physically and logically. | | | | management database. |
| A.12 | Head of ICT | Details of software licences attached to each PC should be held against the asset on the asset register.<br><br>*The Audit exit meeting established that the ICT Section has software that can be used to identify what is installed on a PC. Details of software on individual PC's is kept but not in a composite form. Component Management will be used to bring all this information into one place.* | C | November 2009 | Completed | |
| A.13 | Head of ICT | It should be recognised that with laptops there are security considerations above those associated with a desktop PC. Apart from the potentially damaging loss of data and/or hardware, there are both health and safety and insurance issues to be understood. Guidelines for the secure use of mobile equipment should be drawn up and issued to all laptop users.<br><br>See also recommendation A9. | C | November 2009 | Completed | This forms part of the timetable produced as a consequence of ref. A.3. This will be completed as per the timetable.<br><br>**Anticipated completion date: 27th November 2009.** |
| A.14 | Head of ICT | As the disks have been put beyond use it would be prudent to dispose of these disks through the nominated 3rd party disposal company along with the other redundant IT equipment. This method will be investigated. | D | November 2009 | Completed | All disks are wiped clean by specialist software before being sent for secure recycling. |
| A.15 | Head of ICT | Written procedures should be established to address cases where a virus infection has been identified. | B | November 2009 | Completed | This forms part of the timetable produced as a consequence of ref. A.3. This |

| ***Ref*** | ***Responsible Officer*** | ***Recommendation / Agreed Actions*** | ***Grade*** | ***Suggested Timescale for Completion*** | ***Status as at 15/09/2009*** | ***Tasks*** |
|---|---|---|---|---|---|---|
| | | | | | | will be completed as per the timetable.<br><br>**Anticipated completion date: 6th November 2009.** |

| Ref | Responsible Officer | Recommendation / Agreed Actions | Grade | Suggested Timescale for Completion | Status as at 15/09/2009 | Tasks |
|---|---|---|---|---|---|---|
| A.16 | Head of ICT | A communication exercise should be undertaken to address this situation and inform staff of their responsibilities under the policy.<br><br>*Since the audit, an article about the ICT Security policy has been published in the staff magazine.* | B | ACTIONED | Completed | In addition, a follow up article will be published in the staff magazine on the handling of confidential data. |
| A.17 | Head of ICT | The current situation presents a considerable security risk as it allows for an unlimited number of attempts to guess a particular login password and therefore access the IT network. Accounts should become locked after a set number of attempts. This requirement should be incorporated into any future password policy.<br><br>*Again, this will be resolved once the Microsoft Office and Windows XP rollout has been completed.* | B | November 2009 | Completed | The process of implementing this has begun and will be implemented by the **16th October 2009**. |
| A.19 | Head of ICT | It would be good practice to keep an audit trail of o/s patches that have been released onto the network. | C | November 2009 | Completed | Microsoft Operations Manager (MOM) SUS has been implemented to manage and monitor the release of upgrades and patches. |
| A.20 | Head of ICT | Procedures should ensure that admin passwords are changed on a regular basis or when staff members leave the section. | B | November 2009 | Completed | This forms part of the timetable produced as a consequence of ref. A.3. This will be completed as per the timetable.<br><br>**Anticipated completion date: 21st November 2009.** |
| A.21 | Head of ICT | A record of the UPS and generator tests should be maintained. | C | Immediate | Completed | This will be completed by **24th October 2009**. |
| A.22 | Head of ICT | If the 'Carlisle City Council Staff Email & Internet Policy' (January 2000) has been replaced by the ICT Security Policy document then it should be removed from use on the intranet. Otherwise, the existing document should be reviewed and updated as | C | November 2009 | Completed | This will be completed **by 2nd October 2009**. |

| Ref | Responsible Officer | Recommendation / Agreed Actions | Grade | Suggested Timescale for Completion | Status as at 15/09/2009 | Tasks |
|---|---|---|---|---|---|---|
| | | appropriate. | | | | |
| A.23 | Head of ICT | It would be more user-friendly if the email and internet policies were provided as a separate document as per the document 'Carlisle City Council Staff Email & Internet Policy' (January 2000). See also recommendation A.22. | C | November 2009 | Completed | As the policies are updated this recommendation will be taken into account. |
| A.24 | Head of ICT | Details of legislation relating to the use of the internet and email such as the Data Protection Act and the Computer Misuse Act should be included in the ICT Security Policy. | C | November 2009 | Completed | This forms part of the timetable produced as a consequence of ref. A.5. This will be completed as per the timetable.<br><br>**Anticipated completion date: 27th November 2009.** |
| A.25 | Head of ICT | A link to the Internet Code of Conduct should be supplied on the Internet Compliance Page. The current situation forces staff to agree to a code which they are currently unable to view. | C | Immediate | Completed | This will be completed by **31st October 2009.** |
| A.26 | Head of ICT | Management should assess whether there are legal implications caused by staff not having to sign a declaration acknowledging that they have read and understood either the internet or the email policy. If this policy were to be adopted, the policies and declaration could perhaps be incorporated into the staff induction training.<br><br>*It was agreed at the Audit exit meeting that the Head of ICT will send out an email to all staff asking for confirmation that they know where to find the policies and have also read and understood them. A response from the user's own mail account will act as an electronic signature to confirm this acknowledgement. Users who don't respond may have their internet or email access revoked.* | B | November 2009 | Completed | |

| Ref | Responsible Officer | Recommendation / Agreed Actions | Grade | Suggested Timescale for Completion | Status as at 15/09/2009 | Tasks |
|---|---|---|---|---|---|---|
| | | *ICT should also liase with Personnel to ensure that the above is also covered in staff induction.* | | | | |
| A.27 | Head of ICT | A new risk assessment should be undertaken to identify the risks associated with the internet and email usage | B | November 2009 | Completed | An IT Health Check has been undertaken by an external company to identify security risks both internally and externally. |
| A.28 | Head of ICT | Firewall administration duties should be reviewed. Whilst unlikely, there is still a potential for controls to be exploited without adequate separation of duties.<br><br>*The Head of ICT has agreed to accept this risk.* | N/A | N/A | Completed | |
| A.29 | Head of ICT | Change control procedures should be put in place to govern changes to and administration of the firewall. | B | November 2009 | Completed | This will be completed by **24th October 2009**. |
| A.30 | Head of ICT | A log should be set up to record any changes to the firewall. | C | ALREADY ACTIONED | Completed | |
| A.31 | Head of ICT | The firewall administration passwords should be kept in sealed envelopes in a secure location in case they are ever needed. | C | Immediate | Completed | This will be completed **by 2nd October 2009**. |
| A.32 | Head of ICT | Whilst it is recognised that this is a safety feature, the physical security risk caused by the computer room access door 'failing open' should be reviewed.<br><br>*The Head of ICT agreed that this is a security risk but due to the safety aspect it is a risk he accepts.* | N/A | N/A | Completed | |
| A.33 | Head of ICT | A schedule should be drawn up to review the firewall logs. | C | November 2009 | Completed | This will be completed by **24th October 2009**. |
| A.34 | Head of ICT | An incident file should be set up to record the details of any security breaches and the corrective action taken. | C | ALREADY ACTIONED | Completed | |
| A.35 | Head of ICT | Change control procedures should include website management. All changes should be documented. | C | November 2009 | Completed | This has been included in Ref. A.42. |
| A.36 | Head of ICT | The Accessibility link should be fixed so that it points to the correct location. | C | Immediate | Completed | |

| Ref | Responsible Officer | Recommendation / Agreed Actions | Grade | Suggested Timescale for Completion | Status as at 15/09/2009 | Tasks |
|---|---|---|---|---|---|---|
| A.38 | Head of ICT | Password protected screen savers should be enforced by Windows Group Policy. This would improve security by locking the PC after a set period of inactivity. | C | November 2009 | Completed | This has now been introduced as part of the desktop upgrade. |
| A.39 | Head of ICT | It would be good practice to record the actual date of disposal for IT assets. | D | Immediate | Completed | New Asset Management database has this facility and the disposal date is being recorded. |
| A.40 | Head of ICT | It would be beneficial for ICT staff to have some fire extinguisher training although this recommendation is at the discretion of the Head of ICT. | D | November 2009 | Completed | A number of staff have undertaken fire warden training as part of the building fire planning. |
| A.41 | Head of ICT | Review the classification of data sent off site and ensure that appropriate means of protection e.g. encryption are in place where appropriate. Employees should also be aware of this requirement. | C | November 2009 | Active | All new USB disks include data encryption as standard.<br><br>This task involves more work that initially thought. While the majority of data taken off site has been reviewed, there still remains the task of identifying data taken off-site that ICT Services may not be aware of.<br><br>To be completed by 31st January 2010. |
| A41 | Head of ICT | The ICT security policy should refer users to the Data Protection policy for further information on Data Protection issues. | C | November 2009 | Active | To be completed **by 7th November 2009**. |

| ***Ref*** | ***Responsible Officer*** | ***Recommendation / Agreed Actions*** | ***Grade*** | ***Suggested Timescale for Completion*** | ***Status as at 15/09/2009*** | ***Tasks*** |
|---|---|---|---|---|---|---|
| A.42 | Head of ICT | The IT Section should establish Change Control Standards which adequately cover the following areas:-<br><br>❑ Clarify the roles and define the controls over requesting development and implementation of changes.<br><br>❑ Specify how amendments need to be documented.<br><br>❑ Address planned and unplanned changes including emergency fixes.<br><br>• The following recommendations should also be considered in respect to the Change Control standards:-<br><br>❑ Effective arrangements should be put in place to ensure that the standards are regularly reviewed and kept up to date.<br><br>❑ A copy of the change control standards should be issued to all IT support staff.<br><br>❑ Change Control Standards should include a record of all employees authorised to request program and/or data amendments.<br><br>❑ The Change Control standards should ensure that amendment requests are only accepted if authorised by the system owners or their authorised representatives.<br><br>❑ The change control standards should specify how the amendments should be recorded. | A | November 2009 | Completed | A Change control standard document has been produced, which is currently being reviewed by ICT management before being implemented.<br><br>To be completed **by 30th November 2009**. |

| Ref | Responsible Officer | Recommendation / Agreed Actions | Grade | Suggested Timescale for Completion | Status as at 15/09/2009 | Tasks |
|---|---|---|---|---|---|---|
| | | ❑ A record should be maintained which enables changes to be tracked throughout their life cycle (e.g. version control).<br><br>❑ The possible effects of an implementation should be evaluated including the contingency arrangements required should an implementation fail in the live environment. This could include for example, confirmation that the necessary backups are available or that any scripts used allow the changes to be rolled back.<br><br>❑ Wherever possible, amendments should be tested prior to implementation on the live environment. System owners should ensure they have undertaken adequate testing.<br><br>Any emergency changes should be fully reviewed after the event via an impact assessment. | | | | |
| B.1 | Head of Personnel | Once established, the above policies should be incorporated into the staff induction. A refresh for existing staff members should also be considered. | B | November 2009 but dependent upon ICT producing the policies. | | |
| B.2 | Head of Personnel | See recommendation B.1 | C | November 2009 but dependent upon ICT producing the policies. | | |
| B.3 | Head of Policy & Performance | It would be beneficial to re-commence Data Protection awareness training for all staff who handle personal data. Personnel have agreed to provide the training but this needs to be driven by the Head of | C | November 2009 | | |

| Ref | Responsible Officer | Recommendation / Agreed Actions | Grade | Suggested Timescale for Completion | Status as at 15/09/2009 | Tasks |
|---|---|---|---|---|---|---|
| | | Policy and Performance in liaison with other Heads of Service. | | | | |
| B.4 | Head of Policy & Performance | The Data Protection Policy should be reviewed and updated to ensure it is clear and concise and addresses the following:-<br><br>❑ Explains the need for such a policy<br>❑ States the authority's attitude towards data protection<br>❑ Clearly sets out the authority's data protection requirements<br>❑ States the authority's data protection staffing and reporting structures<br>❑ States the disciplinary procedures which may be invoked should employees fail to comply with the data protection policy<br>❑ Specifically refers to the inclusion of certain structure manual records | B | November 2009 | | |
| B.5 | Head of Policy & Performance | It would be beneficial for the 8 principles of the Data Protection Act to be stated in the policy overview. | C | November 2009 | | |
| B.6 | Head of Policy & Performance | Procedures should be put into place to ensure that in the future, the policy is reviewed annually or immediately in the light of actual events. | C | November 2009 | | |
| B.7 | Head of Policy & Performance | A communications structure should be identified to ensure that data protection issues are effectively communicated throughout the Authority. | C | November 2009 | | |