AGENDA ITEM:

SUMMARY

Report for:	**Audit Committee**
Date of meeting:	**30 May 2012**
PART:	**1**
If Part II, reason:	

Title of report:	**INFORMATION SECURITY UPDATE REPORT**
Contact:	Author/Responsible Officer: John Worts, ICT Team Leader
Purpose of report:	To update Audit Committee on actions taken following Internal Audit report on Information Security.
Recommendations	That Audit Committee consider and accept the update as provided in the body of this report.
Corporate objectives:	
Implications: 'Value For Money Implications'	<u>Financial</u> None arising from this report <u>Value for Money</u> None arising from this report
Health And Safety Implications	

Introduction

In addition to the audit report and derived project plan, I would like to highlight the following areas addressed as part of the wider information security remit.

Policy, Procedures and Guidance

Previously these were located on the Council's Intranet and spread across various locations. The ICT Policies were separated into various technical areas resulting in over thirty different policy documents.

A revamp of the policies was required, and a stronger overarching policy was needed, whilst the disparate technical policies have been combined into one document.

A naming convention will be applied to make it easier to distinguish strategy, policy, procedures, forms and guidance notes.

A stronger security incident reporting procedure has been produced with the relevant prefix DBC999.

The strategy, policy, procedures and guidance notes – will all be place (once approved) in one area on the Council's intranet under 'Documents…Information Management and Security'.

Alongside the relevant corporate policies, I will also place useful hints and tips as well as current alerts for staff and members alike.

Training

I will be running training courses, on all aspects of the information management and security areas including;

- Data Protection Act 1998
- Freedom of Information Act 2000
- Information Security

Courses are scheduled throughout the year, and if any Councillors wish to attend – please contact member support. I would be happy to provide updates or training if required at member development sessions.

Encrypted USB Sticks

115 Council Staff, have been issued with encrypted USB sticks for various aspects of Council business i.e. Emergency Planning, Business Critical and home working.

From the end of November 2012, the encrypted USB sticks will be the only devices recognised on the DBC network.

It would be prudent that any Councillors required a USB stick for Council business, that may contain personal data, be issued with an encrypted USB stick for this purpose.

I will seek advice from member support on the best approach to this.

Herts Forum

Best Practice, dictates that memberships of security forums are advisable, and I attend the Herts Information Security Group – derived from Hertslink ICT. Useful best practice, joint procurement opportunities, policy and guidance are shared at these monthly meetings.

Appendix

INFORMATION SECURITY ACTION PLAN

Recommendation 1: Remote Access Controls (Priority 1)

A review of remote access security controls should be performed with a view to implementing additional security controls for access connections into the Council's network, for example:

- Implementing two-factor authentication controls for remote access to enhance security;
- A policy and process should be established to help ensure that all devices connecting to the Council's network have up to date Anti-Virus and Spyware software in place and that this is regularly updated;
- All PCs accessing remotely should have up to date security patches in place; and
- Restrictions should be established to help ensure that all users are not permitted to download Council data onto PCs unsupported and not owned by the Council.

Management response

Agreed. A policy and process review using best practice on all ICT security practices and policies will be completed by the end of March. Role out of new procedures will also take place to ensure that procedures meet the policy will take place by the end of May.

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
1	**Remote Access Controls**	**Thu 31/05/12**			
	Implementing 2 factor authentication	Fri 30/03/12	**31/07/2012**	ICT	Cryptocard (two factor) has now been deployed, and a decision needs to be made on whether to adopt the AVDC model (Citrix Authentication gateway). I have recommended that two factor still be deployed regardless of authentication model adopted.

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
	Policy developed for updating anti virus software	Wed 29/02/12	**31/05/2012**	Information Security Manager	Revised Policy to be contained within overarching technical security policy
	process for deployment of anti virus software developed and implemented	Mon 12/03/12	**Complete**	Information Security Manager	All endpoint devices now have, Microsoft Forefront Deployed
	SSCM application implemented	Thu 31/05/12	**Complete**	ICT	Microsoft SCCM version 2012 has now been implemented. Information Security Manager, now able to run reports on hardware, software and other asset configurations
	all PC's accessing remotely to have patches	Thu 31/05/12	**30/06/2012**	ICT, Information Security Manager	APG PC's have been audited, and an extension of this audit will be required to encompass PC's at other remote sites, i.e. Housing Wardens

Recommendation 2: **Review of Access to Drives, Directories and Folders (Priority 2)**

Access to network drives, directories and folders should be reviewed and where this is deemed not necessary or required for users' day to day operations, the access should be removed. Where access is required to other departmental shared drives, directories or folders, the reasons for its access should be provided and approved by the information owner of the relevant Department before the access is approved.

Furthermore, a process should be introduced to periodically review the access granted/available to ensure that it is still valid and required for the purpose required.

Management response

Agreed. Procedures for access to drives and access monitoring will be drawn up to ensure the information owner agrees to access being given before access is granted to individuals End of February 2012 completion.

A review of the use of current drives and access to them will take place with changes to access being made subject to the approval by managers. End of June 2012 completion.

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
2	**Review of Access Drives, Directories and folders**	**Fri 29/06/12**			
	Develop procedures for access to drives	Wed 29/02/12	**31/05/2012**	Information Security Manager	Refined through joiners and leavers process
	Ascertain the drive/data owner at Group Manager level for each drive	Wed 29/02/12	**31/05/2012**	Information Security Manager, ICT	Currently waiting on ICT to install reporting software
	Review current access rights included is a refresh of access rights to each drive	Fri 29/06/12		Information Security Manager	See above

Recommendation 3: Laptop Management (Priority 1)

An exercise should be undertaken to identify all Council owned laptops and once identified, an inventory record should be created recording all laptop details. The database should include configuration details such as the make and model of the laptop, version of the software, who it is assigned to and the details of the asset numbering.

Once this exercise has been undertaken, the laptops should be reviewed to ensure that they meet the Council's current security requirements and have hard drive encryption, an up to date and patched operating system and up to date anti-virus software. If the reviewed laptops do not meet the expected standard, they should either be upgraded to the required specification or removed from use.

Additionally, we recommend that all new laptops issued are accompanied by relevant guidance to users such as, the Council's policy on the use and security of laptops.

We further recommend that an annual audit of the Council's hardware assets is undertaken.

Management response

Agreed. An annual review of Council equipment is conducted the last being April 2011. The next review will be over March / April 2012. The inventory will be extended this year to include Software and security running on all laptops and other ICT equipment.

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
3	**Laptop Management**	**Mon 30/04/12**			
	Conduct annual review of Council IT equipment	Mon 30/04/12	**Complete**	ICT Department, Information Security Manager	Will perform quarterly updates using Microsoft SCCM

Recommendation 4: Security of Mobile Phones (Priority 1)

The Council should consider a stronger and robust policy on the issue and use of mobile phones with the need for adequate security to prevent unauthorised access to information (email and data) in the event that the phone is mislaid or stolen.

Management response

Agreed. All phones are password protected ICT completed this work in the autumn 2011. A further review of phone security will be conducted at the same time as the policy review (March 2012). Best practice will be used to ensure that the policy is up to date. Any new processes will then be implemented.

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
4	**Security of Mobile Phones**	**Fri 30/03/12**			
	Review the policy of mobile phones to include security standards	Fri 30/03/12	**End of April - Policy, End of June Encryption**	Information Security Manager, ICT	Phones now have PIN access for emails. Mobile Phone Policy contained within overarching information technology security policy

Recommendation 5: **Password Controls (Priority 2)**

Management should enhance the current password policies for the Corporate Network and for recommended practice within all Council applications. This should require a minimum password length of eight characters to be enforced and restrict the history of previous passwords that can be used to thirteen.

Management response

Agreed. To be implemented immediately

Recommendation 6: Formal user administration and leavers process (Priority 2)

ICT should develop a formal user administration procedure detailing the procedures and processes to be followed for the administration of user accounts. Additionally, a formal process should be introduced for a periodic review of user accounts. In addition, accounts that have not recorded any activity for 90 days should be disabled and any over 180 days should be deleted unless a valid reason has been provided for the account to remain active.

Management response

Agreed. To be implemented as part of the policy review in March 2012.

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
6	**Formal users and administration and leavers process**	**Fri 30/03/12**			
	Process of administration for leavers and users updated	Fri 30/03/12	**31/05/2012**	Information Security Manager	Joiners and Leavers process refined to include more ICT specific requirements

Recommendation 7: Audit Policy Settings and Logging (Priority 2)

The audit policy settings on the Windows network domain should be enhanced by applying the following suggested settings. These events should be reviewed as part of the audit log review process.

Policy Items	Audited Events
Account Management	Success, Failure
Directory Service Access	Success, Failure
Object Access	Success, Failure
Policy Change	Success, Failure
Privilege Use	Success, Failure
Process Tracking	Log failures of process events only
System Events	Success, Failure

Enabling some of these logs may have performance implications on the network and therefore the impact of all changes should be monitored to ensure that they do not have a detrimental effect to the required level of system performance.

Management response

Agreed. Following the evaluation of the effect these logs may have on the performance and the value of the log to GCSx compliance will be made before being implemented. End of July 2012 completion.

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
7	**Audit Policy Setting and Logging**	**Tue 31/07/12**			
	Develop audit logging for the drives in the notes	Fri 29/06/12	**30/06/2012**	ICT, Information Security Manager	Currently seeking to bring supplier in on site for training on product. Logging is done by Windows event viewer.
	Develop a escalation process for anomalies on the reports	Tue 31/07/12	**31/07/2012**	Information Security Manager	Will form part of new Incident reporting procedures.

Recommendation 8: Accounts with Non Expiry Passwords (Priority 2)

A review should be carried out of all accounts whose passwords never expire and controls for these passwords changed to ensure that they are required to change their password in line with best practice.

Should there be an exception where its implementation may affect the operation of the service, this should be documented and its exception authorised by senior management.

Management response

Agreed. A policy on exceptions to passwords will be developed. Some exceptions maybe needed for non-expiry accounts in order to run day to day IT operations. For exceptions a business case will need to be signed off by an Assistant Director. Implementation will be with immediate effect.

Recommendation 9: Use of USBs (Memory Sticks) (Priority 2)

The use of USBs (memory sticks) should be restricted by locking down (configuring) the PCs to only permit approved devices. Where there is a requirement for their use, only Council supplied encrypted devices should be used. Furthermore, we recommend that guidance is issued on the appropriate use of USB devices such as when they should be used and the type of data that may be loaded onto the device.

Management response

Agreed. Corporately enforce the use of encrypted USB sticks of which authorisation will be performed at the Group Manager level. In addition we will prevent access to unauthorised devices. Completion July 2012

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
9	**Use of USBs**	**Tue 31/07/12**			
	USB amnesty to transfer to an approved USB.	Mon 30/04/12	**Complete**	ICT, Information Security Manager	All bar two staff on a list of 115 have now been issued with encrypted USB sticks.
	Locking down PC's to only use encrypted USBs	Tue 31/07/12	**30/11/2012**	ICT	Slipped due to ICT constraints

Recommendation 10: Hardware Disposal Procedures (Priority 2)

We recommend that a formal hardware disposal procedure is developed indicating the acceptable process for hardware disposal. Following agreement, this should be followed for the disposal of all Council equipment.

Management response

Agreed. Asset Disposal policy will be reviewed and changes implemented. Completion March 2012

Recommendation 11: Legal Banner (Priority 3)

We recommend that the Council's Legal Banner on accessing the Council network should be reviewed and updated to include the likely remedial action that could be taken in the event of non compliance with the relevant policies for usage within ICT.

Guidance should be sought from the Council's legal officer for a suitable statement for inclusion.

Management response

Agreed. Review the wording in the login banner against best practice will be completed and implemented. End of February 2012 for completion.

Recommendation 12: Records and Information Management (Priority 1)

We recommend that, as a minimum:

- The current Records and Information Management Policy is reviewed to ensure that it meets with the Council current requirements and usage of data;
- A periodic review is conducted to ensure that users and departments are complying with the policy, for example, on records and data management, retention and destruction;
- An exercise should be conducted to review and remove records that are no longer necessary (in compliance with the DPA) but keeping in mind any regulatory and legal requirements for retention; and
- A documented records disposal procedure should be developed which is available and distributed throughout the Council.

Management response

Agreed. Review of current policy and using of best practice. End of March 2012 completion date.

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
12	**Records and Information Management**	**Fri 30/03/12**			
	Update to the policy new one in place	Fri 30/03/12	**31/05/2012**	Information Security Manager	Still need to revise current policy

Recommendation 13: Data Sharing Protocols (Priority 1)

The Council should review its current approach to information sharing with other government agencies, third parties and private providers. This should ensure that:

- A review is carried out of the data sharing protocols document that is currently in place to ensure it is updated and reflects the requirements of sharing with third party organisations;
- All Departments should be required to formally identify who they share personal data with, the frequency and the form of information that is shared; and
- All users and departments should be advised of the revised protocols and to ensure that they are followed.

Management response

Agreed. Review the Data Sharing protocol documentation and make amendments to the protocol. End of May 2012 completion.

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
13	**Data Sharing Protocols**	**Thu 31/05/12**			
	Review Data sharing protocols around the organisation	Mon 30/04/12	**30/06/2012**	Information Security Manager	Information Sharing Protocols will be assessed, and amendments made where necessary.
	Implement new protocols	Thu 31/05/12	**30/06/2012**	Information Security Manager	

Recommendation 14: IT Policies (Priority 2)

We recommend that a review of all the IT policies is conducted with a view to consolidating and creating an overarching Information Security Policy. Where appropriate, the Council should consider aligning its security arrangements with the guidance provided by ISO27001 the International Standard for Information Security.

Once revised and consolidated, the policy should be approved by senior management of the Council or the IT Governance Board or equivalent.

Management response

Agreed. Develop an overarching policy document for ICT in alignment ISO 27001. Competition March 2012.

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
14	**IT Policies**	**Fri 30/03/12**			
	Review ICT policies	Wed 29/02/12	**Complete**	Information Security Manager	
	Implement one global policy for ICT using Best Practice	Fri 30/03/12	**Complete**	Information Security Manager	To be approved by CMT / Leader for end of May , early June.

Recommendation 15: Security Officer Responsibility (Priority 2)

We recommend that the Role and Responsibility of an Information Security Officer and a SIRO (Senior Information Risk Officer) is formally assigned and the officer appointed is provided with appropriate guidance relating the requirements of the role.

Management response

Agreed. Information Security Role will be defined with in ICT but with links to the Legal Service. Implemented immediately.

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
15	**Security officer Responsibility**	**Wed 29/02/12**			
	Development of Terms of Reference for Governance Group	Tue 21/02/12	**Complete**	Information Security Manager	
	Development of the SIRO	Wed 29/02/12	**Complete**	Information Security Manager	

Recommendation 16: Information Owner and Classification (Priority 2)

We recommend that as part of records and Information Management Policy:

- Ownership of Information should be identified;
- Data and Information classification should be performed; and
- The Council should consider allocating the role of Records Manager to provide guidance on how records within the Authority should be maintained.

Management response

Agreed. A mini audit of the information asset owners will be undertaken. Following this classification of the data and information will be implemented. Completion by the end of December 2012

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
16	**Information owner and Classification**	**Fri 29/03/13**			
	Audit of information asset owners	Fri 28/09/12		Information Security Manager	
	Implementation of classification of the data and information	Mon 31/12/12		Information Security Manager	
	Review of document records management	Fri 29/03/13		Information Security Manager	

Recommendation 17: Security of Laptops (Priority 3)

The Council should consider the issue of cable locks to secure laptops and introduce a policy requiring users to use these when working on any off site location where there are no additional restrictions on entering office locations.

Management response

Agreed. Locks for PC's and laptops at remote sites has started and the role out is due to commence in January 2012.

Recommendation 18: Use of Emails – Monitoring (Priority 3)

We recommend that periodic email monitoring and compliance checks are performed on the use of the Council's email systems to identify any instances of potential excessive usage during core working hours, this information should be routinely provided to management for information purposes.

Management response

Agreed. When this is requested by a senior manager for the team they manage then we will conduct a review.

Recommendation 19: File and Database Protection (Priority 2)

The Council should review the files and folders to certain private and confidential documents stored on remote site PCs and apply protection with the help of IT Services to restrict access to the databases to authorised officers only by use of passwords.

Management response

Agreed. This is part of the encryption and lock down work that is being undertaken currently. Completion for this work is March 2012.

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
19	**File and Database protection**	**Fri 30/03/12**			
	Reviewing data bases and data kept off Civic Site	Wed 22/02/12	**Complete**	ICT	All APG databases and PC's have now been locked down, and access is only via a secure tunnel
	Lock down to meet ICT policy	Fri 30/03/12	**Complete**	ICT	All APG databases and PC's have now been locked down, and access is only via a secure tunnel

Recommendation 20: Archiving of Records (Priority 2)

The Council should review the existing process for storing Council records and especially for Children's data where appropriate documents should be destroyed securely when no longer in use and consideration should be given to scanning documentation to avoid physical copies of data being retained.

Management response

Agreed. Reviewing current polices and ensuring that staff at remote sites are re-trained with regards to procedures on safe data handling.

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
20	**Archiving of Records**	**Fri 06/04/12**			
	Spot checks develop risk register of sites	Wed 29/02/12	**Complete**	John Worts, Noele Pope	Output report for APG produced
	Recommendations implemented from spot Checks	Fri 06/04/12	**Complete**	ICT, Information Security Manager	Follow up report distributed for managers to digest / implement. Follow up site visits to be arranged for June

Recommendation 21: Recycle Bin on PCs (Priority 3)

ICT should provide guidance to staff on how and how often to empty the local PC 'Recycle Bin' to avoid data being retained on Council PCs.

Management response

Agreed. Develop a procedure note to go to all staff on the use of recycle bins and how to delete items from the PC. Completion of this will be the end of February 2012.

Recommendation 22: Data Protection Training (Priority 2)

We recommend that the Council should review the approach used to train Council staff on Data Protection and safeguarding of data to ensure that those users who may process sensitive information are appropriately trained on how to handle personal data. Training and awareness processes should be documented to identify the procedures in place.

Management response

Agreed. The training package has been updated to reflect classification and marking. Completed.

Recommendation 23: Confidentiality and Data Protection Statement (Priority 2)

The Council should perform a review of all data collection forms used to obtain personal information to ensure that these contain a consistent Fair Processing notice. This should be applied to all forms and be approved by Legal Services.

Management response

Agreed. Data collection forms that are used will be obtained from all Group Managers and appropriate fair processing notices will be drafted by Legal Services and returned to Group Managers for inclusion in the forms.

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
23	**Confidentiality and Data Protection Statement**	**Fri 29/06/12**			
	Data collections forms to be reviewed	Tue 01/05/12	**On Track**	Barbara Lisgarten	Barbara currently reviewing all forms
	Implement changes	Fri 29/06/12	**On Track**	Barbara Lisgarten	Barbara currently reviewing all forms

Recommendation 24: Generic use of Email Account (Priority 2)

All users at the Woodwell cemetery should be assigned with personal email accounts for conducting internal Council business, where a generic account is required this should be identified and users should be accountable for use of the generic account.

Management response

Agreed. This will be implemented by the end of February 2012.

Actions Taken/Planned

Audit X-Ref	Task Name	Finish	Revised TT	Resource Names	Progress 14/05/2012
24	**Email Accounts**	**Wed 29/02/12**			
	Review of email generic accounts	Wed 29/02/12	**Complete**	ICT, Information Security Manager	A list of all email accounts has been produced and handed over to ICT