Appendix A

Current and Future Levels of Security against Common Security Threats

Security Threat	Current Position	Future Position
Viruses, Spam & Spyware The introduction of viruses, spam or spyware into the Councils network via any form of media or by using email or the Internet.	The Council deploys up to date antivirus, spam and antispyware software to protect its servers, PCs, laptops and email system. Users are advised to use up to date anti virus, spam and antispyware software on personal equipment when accessing Council systems.	The Council will continue to provide up to date antivirus, spam and antispyware software. In the future users accessing restricted information will do so by using Council provided equipment with up to date antivirus, spam and antispyware software installed.
Data Theft Data leaving the Council from insecure end points such as USB sticks, CD burning	USB use and CD burning is controlled by group policies. An individual can use their own USB stick which current presents a security risk.	End point security will be installed to prevent data leakage. A business case will be required for an individual to be granted use of a USB stick or the ability to burn CDs. The Council will provide encrypted USB sticks in the future.
Remote Access Accessing the Councils systems remotely or from home.	The Council uses Citrix for remote access. There is currently no dual factor authentication in place. Staff can use their own IT equipment. The Council do not have a VPN solution..	A method of using group polices to better control remote access has recently been introduced.Dual factor authentication will be added to further improve security in this area. Users accessing restricted information will do so using Council provided equipment. A VPN solution will be installed.
Third Party Access Allowing access to the Council network by a third party for the purposes of support or software up grade.	Third parties are given a Citrix login which is set to disabled. Access is activated on request and is set to expire after a given time period.	Whilst best practice is being applied in this area, there is a requirement to document this as part of the new security policy. Third parties will be considered as part of the introduction of dual factor authentication.

Firewalls Filters unauthorised dangerous Internet traffic while allowing good traffic to get through.	The Council uses firewalls to protect its data assets. Remote users are advised to use a firewall on personal equipment.	In the future users accessing restricted information will do so by using Council provided equipment with an activated firewall installed.
Downloading Files Using the Internet to download files represent a serious security threat. Many contain viruses or spyware (see above). Clicking "Yes" to software installations in response to pop ups is to be avoided.	The Council uses an Internet & Email filtering solution which prevents the downloading of files and executable programs. By using Citrix, users are not able to install software on PCs. Laptops currently present a security risk. Access to peer-to-peer download sites is blocked.	The Council will continue to use Internet & Email filtering software. A method of locking down laptops will be deployed to reduce the risk in this area.
Using Online Email Using an online email account to access personal email accounts.	Current Internet & Email policy permits users to use their own online email accounts in their own time. Potential backdoor that avoids the Councils filtering solution.	A revised Internet & email policy is being considered by the Council which advises that access to online email accounts be blocked.
The Use of Passwords The use of easily guessable passwords, writing passwords down and the sharing of passwords with others.	Users at the Council have a network logon and password to log on to its network. The password is being toughened to make passwords less guessable inline with GCSX recommendations. Access to individual applications is also controlled by password login. Access to applications and the level of access is controlled by application owners in the user area.	Advice to users regarding passwords will be included in the Councils new Security policy document. The policy will also include guidance covering all areas of security mentioned in this document.
Data Loss Data being deleted and unrecoverable where no data backup has been taken.	The Council back up its core systems and users data on a nightly basis. A proven methodology is applied to each application or data set. Back up tapes are	The backup and recovery process needs to be written into a policy. The introduction of virtualisation and replication as part of a business continuity plan

	taken off site on a daily basis.	will mean that data recovery time will in effect be reduced to 4 hours as replication of data will take place every 12 hours.
Unplanned Change Unplanned changes being made to the Councils infrastructure, software applications or methods and procedures that could increase security risk.	The Council have a change control board with terms of reference that manage change control within IT. It does not include security risk considerations or business impact assessment.	Further refinement of the terms of reference will take place in the coming year to include security risk considerations and impact assessment of any proposed change.