AGENDA ITEM 10

FALKIRK COUNCIL

Subject: **GSX / PSN COMPLIANCE**
Meeting: **EXECUTIVE**
Date: **19 November 2013**
Author: **CORPORATE AND NEIGHBOURHOOD SERVICES**

1. INTRODUCTION

1.1 This report provides an update on GSX / PSN compliance which Members will be aware has been a significant issue for the Council over the last few months. This report outlines the background to GSX / PSN, the requirements regarding compliance, the Councils' immediate response to this and future actions we require to take to ensure continued compliance.

2. BACKGROUND

2.1 GSX / PSN compliance is a significant issue / risk currently facing all UK Local Authorities and many public sector organisations with regards to the way we organise, run and access our IT network. The Council, along with all other Councils, is currently accredited to use the Cabinet Office's secure network called GSX / PSN. We use this network to access such systems as DWP benefit information, to register births, deaths etc. and to communicate with organisations such as the Police etc. by using its secure email system etc.

2.2 The Cabinet Office has recently reviewed their security arrangements for use of GSX / PSN and has advised all users of that network that they must adhere to quite stringent revised security arrangements in order to continue its use, and that Falkirk Council must implement these changes by 4th December or we will be disconnected. This places significant burdens on all users of GSX / PSN to make their networks and equipment more secure prior to and following re-accreditation.

2.3 While only a small but hugely significant part of the Council requires access to GSX / PSN, the new security arrangements apply to the totality of any network that interacts with or extracts information from GSX / PSN. Given the extensive use we make of GSX re DWP, Registers, DVLA etc., we cannot separate out those areas that use PSN from the Council's network. As such the Code of Connection conditions apply to the totality of the Council's network.

2.4 We must establish a trusted network where we have control over what equipment, software etc, who (employees etc.) uses the network and we must apply appropriate and robust security measures to that network. The Council also will have untrusted sites i.e. schools, libraries where the public will use and access the internet but cannot now access our network or use equipment that can access our network. We must separate out those trusted and untrusted sites and keep them physically separate.

2.5 The main areas that require to be secure and trusted are:

- Our network – needs to have appropriate security
- Our equipment – needs to have appropriate security, be registered, owned and supplied by the Council. We also need to make sure it is only trusted users that have access to /use the equipment that links to our network;
- Our people – who access GSX systems or mail, need to be checked and sign a personal security statement. In the first instance this applies to system users with mail users being subject to these terms in 2014.

2.6 Since summer we have, following a robust independent health check, been working with a CLAS consultant (a consultant recommended by the Cabinet Office) to ensure that our network, equipment and people comply with the terms of the code of connection. Given our disconnection date is 4th December 2013 there has been a need to progress our remedial work with a degree of urgency. However, we were strongly advised that we should not submit an application that had not addressed all areas of compliance and indeed those areas specifically highlighted in our health check.

2.7 This has implications for a whole range of areas of our network, our use of mobile equipment and access to the Council's network from home PCs. We must ensure compliance not just at the time of registration but thereafter to ensure we are not found later to breach the code of connection.

2.8 Compliance will continue to impact on the way we do our business. In the time given to ensure compliance we have had to discontinue OWA thus removing e-mail access from a significant number of staff including teachers. This not only affects contingencies for business continuity but can change significantly the way we work in the short / medium term.

2.9 Following a review meeting on the 29 October between IT staff and our CLAS consultant, the Chief Executive signed off our application for reaccreditation on 31st October which was duly send to the Cabinet Office. They will then consider our application and advise us of any areas that we require further remedial action prior to re-accreditation. We are hopeful given the engagement we have had with the CLAS consultant and the remedial actions we have taken that our application will be successful.

3. ACTIONS TO COMPLY WITH THE CODE OF CONNECTION

3.1 While most Councils in Scotland are in the same position with regards to making significant changes to their IT operations to meet these new conditions, the specific changes that have to be made will differ for each Council.

The following action points have emerged as areas we need to address in order to have a reasonable chance of re-accreditation:

- Identify all PSN users subdivided by PSN Service/system users and PSN mail users;
- Excluding untrusted networks (schools, guest networks and public access networks) from the Council's trusted network and therefore from the scope of the code of connection;
- Ensuring that the required corporate security structure is in place. This requires named individuals and responsibilities to be identified in the corporate structure;
- GSX mail to be held separately from the Council's own email system and outsourced
- use of OWA to be discontinued
- Internal VPN solution to be identified (and implemented) – for those on untrusted sites who need access to the Council's trusted network e.g. school administrative staff;
- Implement a firewall white list to allow access to the PSN networks for only those requiring such access; and
- Implement an all managed trusted client (i.e. owned and managed by the Council) remote access environment.

3.2 Some of the ICT services that we currently offer have had to be withdrawn or changed and indeed some others will require to be changed in the near future to ensure continued accreditation. The main changes are detailed below.

Remote access to emails and calendars through Outlook Web Access

3.3 Outlook Web Access is primarily used as a means of connecting to Council email from home computers. The Cabinet Office feels that the level of risk associated with home computers is too great, so unfortunately, access to this service out with Council offices ceased from 31 October 2013.

Access to e-mail on smartphones, tablets etc. i.e. syncing e-mails and calendars etc.

3.4 The Cabinet Office has stated that Council email etc. should not be accessible from mobile devices that are 'unmanaged' (meaning devices which have not had approved and Council supplied security software installed). Currently, our smartphones and tablets do not have this supplied security software and therefore fall into this category.

3.5 We are looking to put in place a plan to enable a secure mobile service to be delivered in the future. However, prior to doing this we had been advised that the Cabinet Office would be issuing guidance on an appropriately accredited solution. That guidance has not been issued prior to us having to submit our application for reaccreditation and unfortunately we are now advised that guidance might not be forthcoming in the near future.

3.6 We had hoped to continue to allow all mobile users to access emails etc. on smartphones until the Cabinet Office had issued further guidance on this. However our CLAS consultant has advised that this will not be acceptable and that we must ensure that any devices we have are encrypted and provided with strong passwords until a more permanent mobile device management solution can be purchased.

3.7 As such the use of e-mail on WindowsPhone 7 devices will be switched off from the beginning of December. Push e-mail will be available (only for non-PSN e-mail) using encryption with strong passwords on WindowsPhone 8 devices. This will be implemented and managed using Microsoft Exchange group policy. Devices will be authenticated to individual mail accounts. Active sync will be disabled by default. This work will be done by 4th Dec 2013. We have identified all essential users and will ensure they are provided with the necessary equipment and security by the due date. However it should be noted that this comes with the need to have strengthened passwords etc. for all users.

3.8 The medium term action must be to implement a compliant MDM solution by end of March 2014, by which time the Council will have identified a solution and confirmed the chosen platform. The Council has been in discussion with several of the MDM suppliers and also with our current mobile telephony service provider. A specification is being drawn up at the moment to take account of not just our current needs but our future needs too e.g. extended mobile working.

3.9 By purchasing a complaint MDM solution we will be able to look beyond existing mobile devices and look to introduce other mobile solutions including potentially tablets.

3.10 It must be stressed that only equipment provided by the Council should be used to access our network so no one should try to access the Council network on unauthorised equipment. To do so would jeopardise compliance with the code of connection.

Classroom access to emails

3.11 We have been advised that it is not permissible to allow access to falkirk.gov.uk email, or indeed the Council network, from PCs which are in an untrusted environment. This would include classrooms. However, we are going to provide an alternative (out of scope) mail system for use in classrooms at which point we will limit access to falkirk.gov.uk mail to the areas of schools where there no children are present.

3.12 Given the need for teachers to access work at home and in the classroom, we need to look at separating them from the Council's network as a number of authorities in Scotland have already done.

Separation of GSX / PSN mail

3.13 In order to continue to use GSX mail we need to separate out such mail from our current email solution. To do this we have given the Cabinet Office the commitment that we will separate PSN mail from our internal mail (and mail server) by implementing the Vodafone managed PSN mail solution. This was outlined in a briefing for Group Leaders that took place a couple of weeks ago.

3.14 A delay in implementing this has occurred because Vodafone was seeking authorisation from GPS for firewall access on Falkirk Councils behalf. This is now estimated to be completed by the end of Dec 2013. We have asked services to provide information on GSX mail users and will be looking to implement the new mail system and provide supporting guidance by the end of the year. We will know the cost of this in the next couple of weeks.

3.15 We understand this is a solution that all Scottish Authorities are considering implementing, so in the future there may be scope to procure such a system on a Scottish basis. Time has not allowed this to take place this year.

Equipment

3.16 We will also be working with services to ensure essential users also have access to secure equipment at home etc. For all other staff this facility will no longer be available. Services have provided us with a list of essential users. It is important to note that we will only allow remote access to users listed by Services and who have authorised equipment.

Networks

3.17 In addition to looking at equipment and users, a significant amount of work has been undertaken by the network and infrastructure team to ensure our network is compliant. The team have moved over 20 sites from one part of the network to another i.e. from trusted to untrusted or vice versa. They have established virtual private networks in a further 5 sites. While there are still one or two pieces of work that need to be completed i.e. public Wi-Fi access in some buildings, much of this work has been done without any disruption or any significant disruption to services.

4. FUTURE WORK

4.1 As noted in the section above while a significant amount of work has taken place to ensure compliance prior to submission of our application, we have a number of significant areas where we need to install permanent solutions if we are to continue to be complaint with the Code of Connection. These in summary include:

- Externalising GSX Mail, developing guidance for staff on this and then ensuring all users have appropriate checks and PSS signed;
- Moving teachers and classrooms out of scope i.e. taking them out of the Council's network;
- Installing a robust permanent MDM solution with associated devices and equipment;
- Reviewing our acceptable use policy and information security policies to reflect the changes we have made;
- Putting in place arrangements to check /audit equipment used to access the network remotely to make sure it complies with our security requirements; and
- Finalising our network arrangements.

4.2 While some of this work will be carried out as a matter of course, there are areas that will require significant spend. At this time it is not possible to give Members a final cost but we estimate that, for example, a robust and secure MDM solution may cost in the region of £200,000.

4.3 Given the potential significant cost and the urgency by which we need to achieve these solutions, we would propose that we use existing budgets i.e. capital and revenue to purchase the necessary software, hardware and equipment. This would mean using underspends from the central ICT budget and also diverting existing capital allocations from proposed replacement programmes. We will also potentially have to use some of the Education ICT capital budget to address the issues of separating schools from the Council's network.

4.4 On one positive note, hopefully the procurement of a robust MDM will allow the introduction of other equipment such as tablets.

5. CONCLUSIONS

5.1 It is important to note that all Local Authorities across the UK are affected by these changes to a greater and lesser extent. We are working with colleagues in other Local Authorities to help the Cabinet Office understand the full impact and to understand some of the solutions they have found to some of the issues noted above that will allow us to re-establish some of the services you currently receive.

5.2 We hope our application shows that Falkirk Council has a genuine desire to ensure compliance with the Code of Connection. Our principal priority has been throughout this process to minimise the risk of a non-compliant application. This approach has meant significant work by the Council on addressing fully the areas highlighted in our health check, significant engagement throughout the process with our CLAS consultant and, importantly, clarity of what we are trying to achieve throughout the organisation. We also understand the impact this is having on services.

5.3 We have taken this opportunity to engage all services with regular updates as well as meetings with relevant staff. In addition we have stressed the need to ensure the principles of the code of connection are understood and adhered to. It must be remembered that while the focus has been on getting reaccreditation, we must ensure continued compliance with the code of connection.

5.4 We understand that with PSN accreditation comes the need for the Cabinet Office to ensure that as a connected organisation we meet the agreed standard. We have through our work to date substantially tightened our compliance and hope that this gives the Cabinet Office the assurance they need to reaccredit our use of PSN.

6. RECOMMENDATIONS

The Executive is asked to:

6.1 Note the details of the report;

6.2 Authorise Officers to work within existing budgets to procure robust solutions for Mobile Device Management, GSX mail, separation of teachers and classrooms from the Council's network and undertake any other remedial work required to ensure a compliance with the Code of Connection; and

6.3 Ask Officers to continue to provide updates on this to services and Members and also bring an update report back to Executive in January.

….....……..
DIRECTOR OF CORPORATE AND NEIGHBOURHOOD SERVICES

Date: 30/1013
Ref: ABB191113.FC
Contact Name: Fiona Campbell EXT 6004

BACKGROUND PAPERS
NIL