Cabinet
Tuesday 19 November 2013
Item No 7

Information Security – PSN (Public Sector Network) compliance
Report by Hillary Kelly, Head of Customer Services

1 Purpose of Report

This report provides a summary overview of the IT security changes that will require to be made to maintain ongoing compliance with the mandatory Cabinet Office PSN (Public Sector Network) Code of Connection, formerly known as the GSX (Government Secure Extranet), and outlines the implications of these changes.

2 Background

2.1 All UK councils connect to other government agencies through the Public Sector Network (PSN). Within Midlothian this facilitates the processing for Births, Deaths and Marriages, information exchange with the DWP, Blue Badge registration, Tell us Once, Criminal History and Delayed Discharge application access, together with secure email communication with the NHS, Police and Central Government.

The PSN offers the opportunity to benefit from accessing and using shared services across Central Government Departments and the wider public sector, reducing costs and increasing efficiency and security.

To maintain the security and availability of the network and to protect connected parties, agencies must adhere to a Code of Connection (CoCo) which details baseline requirements to be applied in terms of IT operations and security arrangements. This is essential to maintain accountability and trust between those organisations sharing information.

2.2 Each year UK councils are required to self-assess and document their compliance against a number of controls and submit to the Cabinet Office for independent assessment.

As a result of some organisations never reaching the minimum security standard and increased cyber security threats, the Cabinet Office changed the IT operation requirements in May 2013 and introduced a ‘Zero Tolerance’ compliance approach. The result in more controls and the automatic disconnection of non compliant organisations.

3 Action required

3.1 The Cabinet Office has mandated that it is no longer permissible to use personal devices to access PSN connected systems or PSN originated data. This means that all non-Council equipment (personal PC’s, tablets and mobile phones) will no longer be permitted to connect to the Councils corporate network and associated services.

The following services will be directly impacted by this mandate and will require being withdrawn:-

- access to e-mail and calendar information from personal devices e.g. home PC's, personal tablets and personal smartphones. This includes use of Outlook Web Access (OWA);
- e-mail active sync to personal iPads and smartphones;
- connecting to Citrix hosted applications such as Frameworki, file access and intranet via personal devices;
- use of personal devices/home PCs to access documents/write reports etc containing personal, sensitive or confidential information.

These changes will not impact on users with protected/encrypted council owned devices such as Council laptops and Council smartphones.

3.2 Further Cabinet Office controls include the requirement for all those accessing PSN services or PSN originated data to meet the Baseline Personnel Security Standard. This will result in an estimated initial 100 employees requiring a basic Protecting Vulnerable Groups check. The Cabinet Office will shortly be issuing further advice and it is anticipated that this number is likely to be extended.

It is clear that the Cabinet Office is likely to introduce further controls as part of their UK cyber security role and further information is awaited in this regard.

3.3 Timescales for changes

Midlothian Council achieved PSN compliance in April 2013 prior to the introduction of new security controls and the 'Zero Tolerance' approach and initially it was believed that the Council would not be re-assessed for accreditation until April 2014. This would have allowed time for a number of changes which were known to be required. However Cabinet Office has since confirmed that due to the timing of accreditation, the Council are not permitted to wait until April 2014 to achieve full compliance.

Negotiations are ongoing with Cabinet Office in relation to revised timescales. It is fully accepted and acknowledged that there is work required to achieve compliance and much of this is already underway. However, it is important that to emphasise to the Cabinet Office, the significant business impact that a premature switch-off could have, before the adequate alternative solutions are established.

The likely timescale proposed to Cabinet Office is for these services to be switched off around mid January 2014 and it is intended the Council can demonstrate the business case for this.

3.4 Accredited Technical Business Solutions

In applying these necessary controls mandated by the Cabinet Office, it needs to be recognised that the Council already has accredited technical business solutions in place that can be implemented, with the current budget, resources and timescales, e.g.

- Accessing of email and calendar information can be serviced from Council procured Smartphone \ Blackberry;
- Access to the Business critical applications inclusive of files and folders and intranet can be serviced by Council procured and encrypted laptop.

To determine the scale, size and scope of this piece of work Heads of Service/service managers are currently undertaking a review of staff work practices co-ordinated by IT Services, to verify and assess how many users have a genuine business need to work in this manner.

Although Business solutions are available to meet this current change in Cabinet Office guidance the staff resource and timescales required to implement these proposed solutions is significant and will be determined, once firm numbers are known.

Furthermore, the time to train and support users in this new way of working with these business solutions is significant. Evidence from existing mobile users tends to suggest that not all users find it straightforward to work in this way, as some staff require additional support and guidance. There may therefore be some impact on overall performance and productivity for an interim period.

3.5 Business Application updates

There are a number of business applications which, at their current version, fail compliance for PSN. These include the “OLM” Homecare system and E-planning system .

Upgrades to these systems would have been required as part of routine business through time, however the PSN issue has meant that immediate action requires to be taken, to prevent non-compliance.

3.6 Schools access to corporate network compliance

Schools devices that require access to the Councils corporate network and/or business systems will also have to become PSN compliant with the requirements of the Code and therefore will need to adopt the same protocols and procedures applied to the corporate network. All Schools currently have a “.Midlothian gov.uk” email address and therefore they require to be compliant.

The main implication for schools staff will be that headteachers will not be able to access their corporate email from their home pc, which it is known, is common practice at present .
The solution in the short term will be to provide all the headteachers (circa 40) with council smartphones so that they can access and monitor their corporate emails.

4 Report Implications

4.1 Resource

As outlined in 3.4 above, employees with a genuine business need who require to remotely access Council systems can be supplied with a Council laptop and/or smartphone, depending on service requirements. These devices can be provided as part of the mobile and flexible working strategy and the full cost implications for this will be accurately assessed once confirmation of exact numbers are known.

It should be noted there is also a dependency on third party providers' ability to deliver to Midlothian Councils timescales and requirements.

Presently a review of the Business requirements is underway and once completed the precise financial implications will be presented to Council outlining the resources impact for 2013/14 and future financial year.

4.2 Risk

The major risk for the Council is that non-compliance with the requirements of the PSN CoCo will result in withdrawal of compliance certificate, PSN disconnection and therefore significant service disruption will occur.

In the absence of secure remote access to email, users may be tempted to send personal or sensitive information to home email accounts or to copy council information to personal devices using an unencrypted memory stick, which would present a significant information security risk.

Furthermore because users have been afforded additional flexibility in the past, there may be a loss of credibility as these necessary changes will be perceived to be a backwards step.

4.3 Single Midlothian Plan and Business Transformation

Themes addressed in this report:

□ Community safety
□ Adult health, care and housing
□ Getting it right for every Midlothian child
□ Improving opportunities in Midlothian
□ Sustainable growth
□ Business transformation and Best Value
☒ None of the above

4.4 Impact on Performance and Outcomes

Non compliance may impact the Council though service disruption, negative publicity and inability to meets the needs of the citizen.

4.5 Adopting a Preventative Approach

The proposals in this report do not contribute to a preventative approach to service delivery.

4.6 Involving Communities and Other Stakeholders

There is no involvement of communities and other stakeholders in this matter.

4.7 Ensuring Equalities

There are no equalities implications arising directly from this report.

4.8 Supporting Sustainable Development

There are no sustainability implications arising directly from this report.

4.9 IT Issues

There are significant IT implications identified throughout this report.

5 Summary

All UK councils connect to other government agencies through the Public Sector Network (PSN) and must adhere to the Code of Connection. The Cabinet Office has changed the IT operational requirements in May 2013 and introduced a ‘zero tolerance’ compliance approach.

To maintain compliance with the Code, a number of IT changes require to be made, which have significant implications for service users. These include removal of remote access to Council systems from personally owned devices and basic security checks to be introduced for staff accessing PSN hosted services or PSN originated data.

Midlothian Council is heavily dependent on its PSN connection to support key services plus secure email communication with the NHS, Police and Central Government, so secure connection requires to be maintained.

Work is progressing to determine the exact extent of service requirements and a report on the financial implications will be presented at the earliest opportunity.

6 Recommendations

Cabinet is requested to:

a) note the requirement to remove:

i. all remote access to Outlook Web Access from personal (unmanaged) devices e.g. home PC's etc.;

ii. all e-mail active sync to staff and Councillor personal iPads and Smartphones;

iii. remote access to Citrix hosted applications from all personal (unmanaged) devices e.g. home pc's etc;

b) note that the switch-off date for these remote services is anticipated to be no later than mid-January 2014;

c) note that an urgent review is underway to identify additional users who have a genuine business need for a smartphone and/or Council laptop to access Council services remotely, to prioritise these demands;

d) acknowledge the requirement for the introduction of mandatory Personal Baseline Security Standard checks for employees accessing PSN hosted systems or PSN originated data with effect from 01 April 2014

e) note that further security changes may be needed to meet Cabinet Office PSN requirements and that additional reports will be presented as required.

f) Note that a further report on the financial implications will be presented at the earliest opportunity.

Date: 06 November 2013

Report Contacts:
Hillary Kelly, 0131 271 3104, hillary.kelly@midlothian.gov.uk and
Ian Wragg, 0131 271 3037, ian.wragg@midlothian.gov.uk

Background Papers: