Public Document Pack

Policy and Performance - Transformation and Resources Committee

Date:	**Thursday, 3 December 2015**
Time:	**6.00 pm**
Venue:	Committee Room 1 - Wallasey Town Hall

Contact Officer: Andrew Mossop
Tel: 0151 691 8501
e-mail: andrewmossop@wirral.gov.uk
Website: http://www.wirral.gov.uk

AGENDA SUPPLEMENT

5. SECURITY OF ACCESS TO COUNCIL ISSUED DEVICES (Pages 1 - 4)

This page is intentionally left blank

WIRRAL COUNCIL

TRANSFORMATION & RESOURCES POLICY & PERFORMANCE COMMITTEE – 3 DECEMBER 2015

SUBJECT:	**Security of Access to Council Issued Devices**
WARD/S AFFECTED:	**None**
REPORT OF:	**Strategic Director for Transformation and Resources.**
RESPONSIBLE PORTFOLIO HOLDER:	**Cllrs A. McLachlan and A. Jones**
KEY DECISION?	**No**

1.0 EXECUTIVE SUMMARY

1.1 Following the Transformation and Resources Policy & Performance Committee - Work Programme Meeting (4th August 2015) Wirral IT were requested to provide a paper regarding "Security of Access to Council issued devices" for meeting scheduled 3rd December 2015.

1.2 This report details the Central Government IT governance frameworks that the Authority operates within and the some of the IT security controls applied to council owned and issued devices.

2.0 BACKGROUND AND KEY ISSUES

2.1 PSN (Public Services Network) is a Central Government security framework that all United Kingdom local authorities operate within. The PSN initiative is designed to unify the network infrastructure across the UK public sector into a secure, interconnected "network of networks". It creates a single logical network, based on industry standards, and a more efficient Information and Communication Technology (ICT) marketplace for the public sector. PSN compliance allows public sector organizations to access and use shared services across central government as well as the wider public sector. The goal is to reduce the cost of ICT services across the UK government and enable more citizen-centric services to be handled at the local level.

2.2 To achieve the objective of greater sharing of ICT services, PSN has to be an assured network over which government departments can safely share information. PSN helps Wirral save money because we can quickly and effectively share information, e.g. with the DWP (Department for Work and Pensions) when processing benefit claims. As a result any loss of PSN accreditation would negatively impact the Authority's ability to efficiently deliver key services. It is estimated that if Wirral was to lose its PSN connection, the manual processing of benefits claims alone would cost Wirral at least £150,000.00p.a. In addition to benefits claims, Wirral relies on its PSN connection to deliver an increasing number of services including, the

Registrars' service, the Blue Badge service, secure pan-government email (GCSX). Consequently, the UK Cabinet Office requires more accountability and a greater focus on compliance to be placed on connected organizations.

2.3 To consume PSN services the Council must submit to an annual re-accreditation process. The submission covers seven areas (detailed below). Some of these activities are delivered for the council directly by the IT Service and are transparent to most users. The security controls we have in place help to protect Wirral's Information Assets and deliver services to the most vulnerable citizens in the borough.

2.3.1 **Overview of PSN Security Requirements**

1. Operational security
    a. Vulnerability management (patch management)
    b. Secure configuration
    c. Physical security
    d. Protective monitoring and intrusion detection
    e. Security incident response
2. Authentication and access control
    a. Sensible authentication and access control to End User Devices e.g. Laptops, Desktops, mobile phones
3. Boundary protection and interfaces
    a. Firewalls etc.
    b. Web filters
    c. Email filters
4. Protecting data at rest and in transit
    a. Data at rest (i.e. within Wirral Councils IT Infrastructure)
    b. Data in transit (i.e. accessed from outside the Council network or transmitted to another location)
5. User and administrator separation of duty
    a. User Privileges
6. Users
7. Testing security
    a. Regular Independent Penetration Testing/Regular IT Health Checks

2.3.2 **How does this apply to Council Issued Devices?**

IT Controls Implemented on Windows 7 devices include

Control	Description
Device Encryption	To protect data at rest if the device is stolen
Antivirus/Spyware	To protect the device from Viruses and other malicious software
Host Intruder Protection	Protects laptops, desktops and servers against known and emerging exploits, including zero-day attacks.
Data Loss Protection	Protects the device against data loss.
Group Policy	Standardising and controlling access to configurations including desktop, Internet Explorer, Microsoft Office and security settings.

Patching Policy	Ensures that supplier security fixes and upgrades are applied promptly.
End User Privilege	Lowered end user privileges prevent users from altering configurations and compromising the security of the device.
Remote Access	Cisco VPN Client (Secure Tunnel) RSA Security Token (two factor authentication) [1]Captive Portal (Public Wi-Fi in Coffee Shops, Restaurants, Internet Cafe, Hotels etc.)

2.3.3.1 In addition, to facilitate sharing of information with other Public Sector bodies, the Authority has to give assurances that our procedures and technologies are appropriate to protect the 3rd party's information; examples of these include Ministry of Justice eBulk DBS (Disclosure and Barring Service) and The Department for Education Eligibility Checking Service.

2.3.3.2 The Authority must also prove that good IT industry assurance practices are being used in order to comply with other public sector security frameworks including the NHS Information Governance Toolkit. This framework facilitates the delivery of our statutory Social Care duties and will facilitate greater collaboration and information sharing with Health colleagues once the council has a connection to the NHS N3 network (and any successor networks). Wirral is currently applying an N3 connection to facilitate the Wirral Health Care Record Vanguard Health Programme. Wirral is currently awaiting assessment and approval of its Local Connection Architecture document, which demonstrates our management of information risk and includes our technical architecture, IT controls, and procedures. Wirral IT adheres to the Local Public Services Data Handling Guidelines which are a Local Government-tailored version of Central Government guidance issued after the HRMC major information security breach in 2007.

3.0 RELEVANT RISKS

3.1 Poor IT controls may lead to loss of access to external services i.e. DWP Systems.

4.0 OTHER OPTIONS CONSIDERED

4.1 None

5.0 CONSULTATION

5.1 None

6.0 OUTSTANDING PREVIOUSLY APPROVED ACTIONS

6.1 None

7.0 IMPLICATIONS FOR VOLUNTARY, COMMUNITY AND FAITH GROUPS

[1] Captive Portal – Currently Wirral's wireless access is based on Central Government's CESG AP12 Wireless Security Standard which prevents access to captive portals; this includes Public Wi-Fi, Internet Café and Hotel etc.

7.1 None.

8.0 RESOURCE IMPLICATIONS: FINANCIAL; IT; STAFFING; AND ASSETS

8.1 None.

9.0 LEGAL IMPLICATIONS

9.1 Poor IT controls may lead to loss of data and breaches of various legislation, including the Data Protection Act 1998. Each breach (of the DPA) can attract a financial penalty of up to £500,000.00.

10.0 EQUALITIES IMPLICATIONS

10.1 None.

11.0 CARBON REDUCTION AND ENVIRONMENTAL IMPLICATIONS

11.1 None.

12.0 PLANNING AND COMMUNITY SAFETY IMPLICATIONS

12.1 None

13.0 RECOMMENDATION/S

13.1 None

REPORT AUTHOR: Phil Moss, IT Infrastructure Manager

telephone (0151) 666 3868
email philipmoss@wirral.gov.uk

APPENDICES

BACKGROUND PAPERS/REFERENCE MATERIAL

SUBJECT HISTORY (last 3 years)

Council Meeting	Date