Inverclyde
council

AGENDA ITEM NO. 9

Report To: Policy & Resources Committee	**Date: 25 March 2014**
Report By: Acting Corporate Director Environment, Regeneration & Resources	**Report No: ICT 25-3-14 PSN Compliance Update**
Contact Officer: Robert Stoakes	**Contact No: 01475 712765**

Subject: PSN Accreditation Update 2014

1.0 PURPOSE

1.1 The purpose of this report is to update Committee on the current position with the Public Services Network (PSN) Accreditation process and to highlight changes that may be required to allow for continued accreditation.

2.0 SUMMARY

2.1 The Public Services Network provides the Council with secure access to a number of services provided by National, Regional and Local Government departments; Registers of Scotland (Births, Deaths and Marriage records), DWP, Violent and Sex Offender Register (ViSOR) as well as providing secure interdepartmental communications via GSX Email. Each year, the Council is required to accredit its compliance with PSN Code of Connection. The new accreditation process began in April 2012 and Council was awarded its PSN Accreditation on 31st July 2013, thereby granting continued access the secure PSN Network until 1st August 2014.

2.2 ICT Services has begun preparing for the next round of accreditation with the commissioning of the annual IT Health check. ICT is aware of developments and clarifications from the Cabinet Office which will require additional work from the Council for successful reaccreditation.

2.3 ICT Services and the Information Governance Steering Group (IGSG) have identified a number of areas of action that will be addressed as part of the process for re-accreditation. These include further Disclosure Checks, changes to some external web sites, Data Sharing and Mapping and the introduction of Two Factor Authentication for remote access. Work on these areas has been agreed and is underway for completion by the next submission date.

2.4 ICT Services has also identified a number of further changes that **may** be required, dependent on the development and clarification of policies in a number of areas. These will be clarified throughout the year and, at present, none is seen as causing significant difficulty, although all will require resources and time to address.

3.0 RECOMMENDATIONS

It is recommended that:

3.1 Committee note that the Council successfully completed the PSN accreditation process for 2013/2014.

3.2 Committee note that accreditation is an on-going process and that there will be further changes required to Information Security policies, practices, and infrastructure.

3.3 Committee note that ICT will continue to work in conjunction with Services and the Information Governance Steering Group to ensure the implementation of the necessary changes required to maintain the Council's PSN accreditation.

Robert Stoakes
Transitional Head of ICT

4.0 BACKGROUND

4.1 The Public Services Network provides the Council with secure access to a number of services provided by National and Regional Government departments; Registers of Scotland (Births, Deaths and Marriage records), Department of Work and pensions, Violent and Sex Offender Register (ViSOR), as well as providing secure interdepartmental communications via GSX email. Each year, the Council is required to accredit its compliance with PSN Code of Connection. The Council was awarded PSN Accreditation on 31st July 2013 granting continued access the secure PSN Network until 1st August 2014.

4.2 The Cabinet Office introduced a new accreditation process in April 2012 with the publication of a new Set of PSN Standards, Code of Connection Documentation and guidance on a new “zero tolerance” approach to the compliance process.

4.3 The general approach taken by the Council mirrors the requirements set by the Cabinet Office, so the effect on ICT service delivery by the new accreditation process has been minimal.

The core tenets of the process all broadly matched the Council’s approach and infrastructure practices:

- segregated Networks (Corporate, Education and Libraries)
- separate, secure PSN Infrastructure
- separate GSX Mailboxes
- no PSN data to be accessed from outside our core physical corporate network
- no unmanaged devices (BYOD)

4.4 ICT Services has begun preparing for the next round of accreditation with the commissioning of the annual IT Health Check to be completed by May 2014. ICT is also aware of developments and clarifications from the Cabinet Office which will require additional work from the Council for successful reaccreditation. However this is no different from the previous (GSX) regime where the compliance process evolved as new threats and challenges were identified.

4.5 ICT Services and the Information Governance Working Group have identified a number of areas of action that will be addressed as part of the process for re-accreditation. A full Action Plan (Appendix 1) has been developed and work is underway to review requirements, implement any changes and introduce new policies required to support continued PSN compliance. It should be noted that not all actions require to be completed for the 2014 assessment.

4.6 Further Policies and Procedures may need to be developed to manage the flow of data used by Elected Members to ensure “official” Council information is not forwarded to home email addresses or stored on home or personal devices.

4.7 The “zero tolerance” approach taken by the Cabinet Office means that there is now no leeway in the compliance process. If a service identifies and proposes a new way of working which would have an impact on the accreditation process, they must be aware that the costs to ensure compliance must be funded from within the project.

4.8 In particular, any significant changes to the Council's approach to agile working or any consideration for data sharing must be carefully considered and may require the use of significant external resources to ensure that the network design and infrastructure is provided in a secure and sustainable way that meets compliance requirements. Advice from SOCITM continues to be that Councils should refrain from planning or implementing any form of BYOD initiative until the Cabinet Office has completed its recommended design strategy.

4.9 A new Government Classification Scheme (GCS) replacing the existing Government Protective Marking Scheme (GPMS) will be introduced in April 2014. Indications suggest that the approach will be much simplified with the majority of data generated by the Council simply known as "Official" this should streamline how data is managed within the organisation.

5.0 IMPLICATIONS

Finance

5.1 Financial Implications. Potential additional costs are unknown at present. This will be clarified once the Council's annual ICT Health Check has been completed and an action plan agreed. At this point in time it is not envisaged that there will be any costs that cannot be contained in approved budgets.

CMT has agreed to fund the one-off costs of the Disclosure Scotland Basic Disclosure Check requirements of the Baseline Personnel Security Standard. It is anticipated that circa 1200 employees will require Basic Disclosure Checks at £25 per employee plus administration costs (£30,000 + £15,000). These costs are to be met from earmarked reserves.

One-off Costs

Cost Centre	**Budget Heading**	**Budget Years**	**Proposed Spend this Report**	**Virement From**	**Other Comments**
			To be confirmed		

Annual Recurring Costs / Savings

Cost Centre	**Budget Heading**	**With Effect From**	**Annual Net Impact**	**Virement From (if applicable)**	**Other Comments**
			To be confirmed		

Legal

5.2 There are no Legal implications.

Human Resources

5.3 There are new requirements related to safe recruitment processes that HR/OD are progressing.

Equalities

5.4 There are no equalities implications.

Repopulation

5.5 There are no repopulation implications.

6.0 CONSULTATIONS

6.1 The Cabinet Office is responsible for managing PSN Compliance for all local authorities. ICT consult fully with the allocated PSN Project Manager at The Cabinet Office.

6.2 SOCITM, the professional association for ICT Management, is working closely with The Cabinet Office on a number of aspects of the compliance process. ICT is liaising closely with SOCITM as this progresses.

6.3 PSN Scottish Design Workshop, the Council has been invited to work with other Las to design solutions for common issues affecting all PSN certified agencies.

7.0 BACKGROUND PAPERS

7.1 None.

Appendix 1 – PSN 2014/2015 Action Plan

Section 1 – Physical Security			
Control	**Detailed Requirement**	**Action Required**	**Target Date**
The connecting organisation shall ensure that physical access to buildings and rooms holding PSN equipment and terminals are secured.	Where a council or department uses PSN Services, the Server and Network Cabinet must be locked and the keys must be stored and controlled centrally by ICT. If possible the Cabinet must be in a locked room that only IT has access to (at the very least it must not be accessible except for custodial/security staff). Existing Hub rooms will no longer be permitted to be used for storage of non ICT Equipment.	Review all current ICT Cabinet Locations, confirm security requirements. Liaise with sites regarding security in hub rooms.	Site Surveys to be completed by 1st October 2014
	Security enhancements to ICT hub rooms and network cabinets in locations out with Greenock Municipal Buildings. This will impact locations such as schools where hub rooms will no longer be permitted to be used as storage by the schools. Where necessary, additional security such as code locks will need to be installed – access will also have to be restricted to ICT Staff only.	Review Comms & Hub rooms in all Schools and remote locations – remove all non ICT equipment.	Site Surveys to be completed by 1st October 2014
	We will need to implement key controls to the cabinets in remote location - discuss with Servicedesk requirements etc.	Replace locks and doors where required	Site Surveys to be completed by 1st October 2014
	All PSN Services should be co-located in a separate and physically secure cabinet	Relocate PSN equipment to secure cabinet in Data Centre	10th Jan 2014 - Completed
Section 2 – Personnel Security			
Safe Recruitment/BPSS	The customer shall ensure that any user, supplier or 3rd party involved in the consumption or provision of PSN Services receives appropriate security vetting. The vetting standards shall be based on the Baseline Personnel Security Standard (BPSS) or comparable	OD&HR have updated the Council's Safer Recruitment Policy to ensure compliance with BPSS	1st Feb 2014 - Completed
	– OD&HR To review all existing employees and ensure Basic Disclosure Scotland Checks are completed for all staff by August 2015	OD&HR have begun the disclosure process for all staff	1st August 2015
	Confirm details of PSN System users and confirm ongoing access requirements	Access confirmed for all PSN applications (BBIS, DWP, ViSOR) - ongoing work to confirm GSX Mail users.	1st April 2014

	Third Party Users – all third party contractors and support staff will require to meet BPSS standards to work on any council system that can access the core Corporate network	Liaise with procurement to ensure requirement is included in general terms and conditions	1st June 2014
Section 3 – Data Sharing and Mapping			
PSN Originating Data	It is a condition of access to the PSN that data originating from that source (PSN Originating Data) is treated with an appropriate level of security. It is forbidden to forward PSN originating data onto a less secure environment e.g. devices on the Schools Network or at home without the explicit consent of the data owner. Policies must be refreshed to ensure employees are aware of this restriction.	The IGSG has implemented a number of initiatives that will ensure compliance with this process. Information Asset Owners will be nominated for each service.	31st October 2014
Data Mapping	An exercise to model the flow of traffic from PSN systems to ensure that they are understood and that no sensitive data is being copied onto insecure or otherwise inappropriate locations. Work being undertaken by the IGSG to implement an Information Asset Register and identifying Data Owners will be key to ensuring compliance with this requirement	As part of the Data Mapping exercise being carried out by IGSG all Data owners are being asked to identify Data Flow and Mapping.	TBC – following identification of Information Asset Owners
Data Sharing	The Information Governance Steering Group has recently reported to committee progress on robust data sharing agreements must be established with partner agencies to ensure that other organisation know exactly what actions can be taken with data sent to or from the Council. Work being undertaken by the IGSG to consolidate and enhance Data Sharing Agreements will be key to ensuring compliance with this requirement	IGSG Managing data sharing and use agreements.	TBC – following identification of Information Asset Owners
Secure data in Schools	There will be an increasing requirement to process sensitive data within schools and other educational establishments. It is likely that we will need to increase the number of corporate workstations available for use by teachers to provide a secure network environment in which to send, receive, record and process sensitive information about pupils.	ICT Services are initially responding to requests on a case by case basis. Longer term there will be a requirement to review the data stored on school networks	TBC
Section 4 – Remote Access			
Implement Aventail	2 Factor Authentication (an additional form	Implement	11th June

Tokenless 2FA	of identification) will be required for all remote access to the Corporate Network. ICT has begun the work required to implement this requirement, utilising a facility within our existing SonicWALL Aventail SSL VPN and this work will be complete by the reaccreditation date. A unique 4 digit pin will be sent by SMS text message. This will be entered as part of the login process.	Aventail Tokenless 2FA, Create User instructions and implement changes.	2014
Home Working	There is still anecdotal evidence of staff emailing work to personal accounts to complete on their home/personal PCs. As there is no way to securely manage these devices and ensure that they are virus or spyware free, the Council must reinforce, with suitable sanctions, the current policy that forbids using home PCs for official purposes.	Remind all staff of current Acceptable Use Policy.	1st June 2014
PSN Access	It will still not be permissible for PSN Services to be accessed by remote devices	Controlled by Firewall Rules to prevent onward transmission of data	1st February 2014 - Completed
Authentication	It may be necessary for a unique username and password to be used to log in to the network from an external location(i.e. independent of normal log-ins)	Clarification to be issued by Cabinet Office	Awaiting advice from Cabinet Office
Device Security Settings	it may be necessary to implement further security enhancements on smartphones and PDAs. This may include restricting access to services and applications that are not managed by the Council.	Review Exchange Settings - business requirement for cameras etc. for individual staff groups.	1st May 2014
HTTPS Authentication	Access to VPN via a secure/encrypted web connection	Completed – staff redirected to https: URL	1st Dec 2013 - Completed
Firewall Configuration	Amend configuration to support AP2 – walled garden	Minor network change required – will require downtime for remote network users	17th May 2014

Section 5 - Configuration			
External Web Services	HTTPS and authentication will be required for any secured web sites and services. This will require an update to the online Planning System to reinstate online comments. This work has been agreed with the service and will be complete before the reaccreditation date.	Discussions ongoing with supplier	1st June 2014
Managed Endpoints	Only devices owned, supplied and fully managed by the Council will be permitted to be attached and to access the Council's Corporate network. This will have implications for guests who will no longer be permitted to use their own laptops/notebooks on the Council network. The RVJB Staff within the Contact Centre will need to migrate to a Council-managed PC to access their systems. Solus screens and NHS PCs and notebooks will not be allowed to access Council IT systems (Although the current approach of allowing NHS staff to use Council systems to access NHS applications can continue)	The council had previously allowed guest access to internet services via wired or wireless network services. This will no longer be permitted	10th January 2014 - Completed
Endpoint Security	No Mobiles to be connected via USB for charging/synchronisation. All connectivity to the council network via Aventail - attaching personal devices (iPods, iPhones and other personal mobiles) to corporate PCs for charging is seen as a security risk, as there is a possibility that the device could be compromised and present a security risk to the host device. This practice will need to cease	Updated advice to be issued to all staff – ICT will review system reports to identify devices attached to council equipment.	1st July 2014
Review group policies for Windows 7	Follow guidelines at: followinghttps://www.gov.uk/government/publications/end-user-devices-security-guidance-windows-7-and-windows-8	Update group Policies where required	1st March 2014 - Completed
Review general guidance for End User Devices	Follow guidelines at: https://www.gov.uk/government/publications/end-user-devices-security-guidance-enterprise-considerations	Update group Policies where required	1st March 2014 - Completed
Review Wireless Network Configuration	Review existing Wireless configuration against AP12. Confirm existing restrictions including access to PSN Services via a wireless LAN	Update configuration as appropriate	3rd March 2014 - Completed
Section 6 – Secure Email			
GSX Email	This system must only be used for receiving or sending data to other external secure email systems. The practice of using GSX mail for internal mail will no longer be	Updated advice to be issued to all staff – ICT will review system	1st August 2014

	permitted. Updated user guidelines will be issued to staff.	reports to identify internal email or non-secure email.	
GSX Email	GSX Email - It is likely that we will need to move away from the current Lotus Notes-based GSX Email system as this moves out of support. A number of cloud-based secure email services are available via G-Cloud and it is anticipated that ICT will look to this solution.	Likely date will be mid-2015 ICT will investigate options.	1st June 2015
Section 7 – Unsupported Applications and Systems			
MS Windows XP and Office 2003	There is a requirement to migrate from our current Windows XP Operating System and MS Office 2003 Office suite, as they will no longer be supported by Microsoft from April 2014 and it is a requirement of the PSN process that all systems and applications are fully supported and receive regular security and functionality updates from the manufacturer. A project to update all PCs on the Corporate network has been implemented and is well underway	ICT Services are currently mid-way through a refresh programme to upgrade all corporate PCs to Windows 7 and Office 2010	1st August 2014
Legacy Applications	All applications and systems on the Corporate Network must be fully supported and be receiving security and system updates. A number of systems have been identified that will no longer be permitted to be used and we will work with system users to provide alternative, fully supported systems.	Discussions ongoing with a number of services to ensure a smooth migration to supported applications.	1st August 2014
Section 8 - Policy & procedures			
Security policy Framework	The Government Security Policy Framework (SPF) will continue to provide the overall template for the Council's approach to ICT Security, although greater emphasis will also be given to supplementary Good Practice guides and Architectural models published by the Cabinet Office.	Review SPF to ensure continued compliance/alignment of local ICT Security policies with national standards	1st March 2014 - Completed
Network Security – IL2	The Scottish Government and the Cabinet Office have agreed to the recommendation that Scottish Local Authority ICT networks should be redesignated as Impact Level 2 from Impact level 3 – bringing Scottish LA's in line with other UK counterparts.	Awaiting change process from Cabinet Office.	1st June 2015 Estimated
AUP	An updated AUP will be required to reflect and enhance the current security framework.	ICT and the IGSG to produce updated AUP for	1st August 2014

		Committee approval	
Protective Marking	Introduction of the new Government Security Classifications	Update Council Scheme to reflect GSC – IGSG to review	TBC
Network Diagrams & Scope	A high level/logical network schematic shall be provided	ICT To Produce Updated Diagram	11th June 2014
Remote Access network Diagrams	Provide Network Diagrams showing Dell SonicWALL Aventail design.	ICT To Produce Updated Diagram	11th June 2014
Section 9 – IT Health Check			
Organisations shall implement an annual programme of IT Health Checks to validate equipment not provided as part of a PSN service that interacts with PSN services.	Third Party Penetration test to be commissioned and completed by 1st May 2014 Order placed & test scheduled for March/April 2014	Order placed & test scheduled for March/April 2014	1st May 2014

Annex B - Glossary of Terms and Abbreviations

2FA	2 Factor Authentication; A two-step verification process to verify the identity of a user on a remote device such as a laptop or tablet.
AP2	Architectural Pattern 2 - UK Government approved internal network design for remote access to official system
AP11	Architectural Pattern 11 – UK Government approved network design for mobile remote access of official systems
AP12	Architectural Pattern 2 – UK Government approved network design for enterprise wireless networking.
AUP	Acceptable Use policy – Council policy governing use of ICT Systems.
BPSS	Baseline Personnel Security Standard – Foundation level of employment screening required by UK Government
BYOD	Bring Your Own Device – use of personally owned devices to access official information.
CESG	Communications-Electronics Security Group - The UK Government's National Technical Authority for Information Assurance (IA). Part GCHQ
CoCo	Code of Connection – Accreditation agreement and document detailing our responsibilities towards Information Assurance and ICT Security
GCHQ	Government Communications Headquarters – British Intelligence Agency responsible for UK Government Information Assurance
GCS	Government Classification Scheme – Document marking/classification scheme to be implemented on 1st April 2014
GCSX	Government Secure Extranet – UK Government secure interdepartmental network classified to Impact Level 2
GSX	Government Secure Extranet – UK Government secure interdepartmental network classified to Impact Level 3
GCSX	Government Secure Extranet – UK Government secure interdepartmental network classified to Impact Level 2
GPMS	Government Protective Marking Scheme – Current document marking/classification scheme – to be replaced on 1st April 2014
IL2	Impact Level 2 – Data up to the level of PROTECT under GPMS. Now no mapped link between IL and GCS
IL3	Impact Level 3 – Data up to the level of RESTRICTED under GPMS. Now no mapped link between IL and GCS
ITHC	IT Health Check – review by third party/external consultancy of the Councils ICT Systems and Network.
Legacy System	System retained for historical records or services – no longer supported by supplier.
PSN	Public Service Network
SoCITM	Society of IT Management – Professional body representing IT Managers primarily in the Public Sector or who deliver services for public benefit.