National Assembly for Wales Commission (Assembly Commission)

Shared Network – Assembly Members and Assembly Staff

1. Background

The Assembly is currently part of the Government Secure intranet (GSi). This network enables public authorities to exchange and share restricted (and confidential) information with other GSi community members. Other GSi services used include secure access to the public internet plus anti-spam and anti-virus scanning for staff. There is a logical and physical boundary between the networks used by Assembly staff (HF domain) and Assembly Members (BF domain) and due to the restrictions of operating within GSi, difficulties arise when sharing information between the two networks, preventing direct access for BF domain users to HF resources. To improve services and the flow of information between the two organisations, a unified network on which Assembly Members and Assembly staff reside is key. It should be noted that some existing occupants of Tŷ Hywel would remain on GSi; namely Ministers, Cabinet Office and the Welsh Assembly Government Press Office.

Data circuits to constituency offices are provided through the Merlin contract and the current recommended product is managed via Merlin. The speed at which this operates is set conservatively to ensure high availability to the office; however, it prevents the use of technically faster and cheaper solutions provided by alternative suppliers. The infrastructure design is based on traditional application, file and print services with large amounts of data currently being passed between locations, causing bottlenecks.

2. Options

One option would be to look at the different technologies that are available to a constituency office and ensure the best available and best value technology is applied to that office (more detail is available in **Annex A)**.

A number of services are shared between the Government and the Assembly. Primarily, these are: Internet access, file and print, directory services and application servers, including email, database and intranet. A move off GSi would mean that these shared services would need to be replicated on the new network, designed and any new hardware purchased. Obvious benefits of moving Assembly staff to the Members' network exist and the infrastructure is sufficiently sized to allow this. The existing granular security would remain to ensure that current control and access to files and information is still held by nominated party Members; Assembly staff would not be able to access this data unless explicitly granted by the P drive administrators. To reduce the cost of separating the two organisations, moving onto the Members' network would allow us to utilise existing assets and reduce the need for hardware duplication. This would significantly reduce any capital expenditure, and the cost per user of the infrastructure.

2.1 Implications of staying on GSi

The GSi network provides a very controlled and therefore stable infrastructure. However more flexible working methods, in line with the Assembly's strategy, would be restricted and costly to implement, with limited benefits.

Within GSi the Assembly's ability to react to business change is slow, therefore early momentum can be lost on projects.

Some of the ICT services that people take for granted at home or elsewhere would remain restricted, e.g. USB ports, web mail, personal video conferencing, access to the Assembly's systems from personal PCs.

2.2 Implications of moving off GSi

Internal processes would need to be put in place to ensure that the network is managed in accordance to any new Assembly Code of Connection – these are currently provided by the Government.

As previously mentioned, there would still be remaining GSi users in Cardiff Bay, therefore it would still be necessary to ensure all the physical controls required for GSi accreditation were maintained.

A transition period would need to be managed for the business change of email services as the Assembly would no longer be part of @wales.gsi.gov.uk.

Information flow between Members and Assembly staff would be facilitated due to user accounts and groups residing within the same security boundary.

Currently, it is not possible to give BF users direct access to HF resources (file shares, intranet).

There is the potential for an upgrade of the Members' infrastructure to handle an additional 300+ Assembly users.

Physical separation of the GSi infrastructure is difficult to achieve between Ministers and Members within the accommodation constraints of the Senedd.

3. Technical steps to separation

3.1   Typical high level task

The detailed requirements of separating Government staff and Assembly staff will need to be captured, although the use of the Members' domain will ensure value for money is maintained, whilst implementing a strong network.

The key stages can be defined as:

- Identification of Assembly staff user data from the current network infrastructure;

- Check the existing BF network topology to ensure infrastructure is suitable for additional users, make any changes as necessary, including upgrades where required;

- Review and present findings on Wide Area Network (WAN) connectivity between Cardiff Bay and constituency offices, including internet access;

- Review core systems used on BF with the aim to provide a clear migration path to newer versions of the applications, typically email and intranet;

- Make any changes required to Siambr systems;

- Implementation of application servers into a new domain, where required;

- Reconfiguration of network infrastructure from HF into BF domain, including any changes for Members' connectivity improvements;

- Decide on an appropriate build for Assembly staff PCs – thin or rich clients;

- Migrate data into new environment using existing BF server hardware or upgrade where appropriate;

- Migration of computer and user accounts into a new domain.

3.2 More detailed low level tasks

Some additional tasks will be required, both on the internal Local Area Network (LAN) and the WAN, to ensure security prevails and, where required, improvements are delivered. These include:

- Re-patch access switches to connect to BF Cisco routers in Tŷ Hywel and Senedd;

- Add additional cards to routers to connect all access switches;

- Reconfigure access switches to use BF Virtual LAN;

- Ensure that proxy servers can handle extra level of network traffic; however the Assembly have recently invested in this area.

- Tender for our own internet facing links at a possible configuration of 2 x 40Mb (dual redundant and resilient circuits), possibly at a cost of £40,000 per annum on 3 year contract;

- Investigations on the infrastructure (DMZ implementation / upgrade) to prepare for web enabled applications (possibly at £20,000)

- Task list for server infrastructure to be agreed;

- Domain controllers to be reviewed to ensure compatibility and resilience;

- Move staff P drive data over to new Storage Area Network (SAN), which will require an additional amount of storage space, possibly 500Gb;

- Reconfigure P drive permissions, create groups, log on scripts as required;

- H drives and profiles to be changed;

- Exchange servers implemented as appropriate, with additional cluster for Assembly staff;

- Mailbox migration plan to be developed, tested and agreed, then scheduled as appropriate for the project, probably around creating a personal folders (.pst) file and then importing into BF;

- The intranet can either be moved to a new server, or if time allows, a new application introduced. This will require technical and operational resource;

- Structured Query Language (SQL) server for MRS moved to the BF domain, possibly to a new application cluster, details to be agreed;

- Assembly applications are also required to be migrated. e.g. FTR Gold/Deja vu/Filenet, in line with SQL server;

- Anti Virus, security patches and Managesoft can remain under the current protocol;

- Investigations can be undertaken and, if necessary introduced, on improving the back-up infrastructure, this meets growing data storage requirements – possibly add new tape drives (2 x LTO4 at £12,000 each);

- The HR and Finance systems (Snowdrop and CODA) plus the Assembly websites are all externally managed services, and can remain. Checks will be required on access routes and permissions;

- Migration of Assembly staff BlackBerry devices to Members' BlackBerry contract;

- Checks will be required on the Backhaul Extension Service, to ensure it can handle additional BlackBerry devices.