Comisiwn y Cynulliad
Assembly Commission

NAFWC 2010 (Paper ~~x~~ 7 Part 1)
ICT Security Usage Rules

Cynulliad Cenedlaethol Cymru
National Assembly for Wales

Date: September 2010
Time:
Venue:
Author name and contact number: Brian Davidge, ext 8879

ICT Security Usage Rules

This paper has been prepared for consideration by the National Assembly for Wales Commission. It has been deemed suitable for publication after such consideration in line with the Commission's rules for conduct of business. Premature publication or disclosure of the contents of this paper is not permitted as this might prejudice the Commission's deliberations

1.0 Purpose and summary of issues

1.1. With the implementation of the new Assembly ICT infrastructure (UNO) a new set of ICT usage rules have been drafted.

2.0 Recommendations

2.1. To note the new ICT usage rules.

3.0 Discussion

3.1. The new Assembly ICT infrastructure designed and implemented as part of the UNO project gave the Assembly, for the first time, a single ICT network, used exclusively by Assembly Members, their support staff and Assembly staff.

3.2. To coincide with the merging of the Assembly Member and Assembly staff networks, a new set of usage rules have been drafted. As Members, support staff and Assembly staff will be sharing a network, they will also share a security policy.

3.3. Whilst a key benefit of UNO is flexibility, we still need to ensure the network is secure and that the Assembly continues to have a

duty of care to users on that network. These usage rules have been drafted using the rules previously in place on each domain and are designed to meet the strategies of the Assembly and the many policies that exist, including any changes brought about under the recommendation of the Independent Panel. As such, users will not see many changes from previous policies.

3.4. A review of the main differences between the previous rules and the new rules is shown in annex 1.

3.5. These rules have been written with the help and guidance of the UNO project board; the UNO users group (made up of Assembly Members' support staff and Assembly staff); HR; trade union officials and the Commissioner for the Assembly and the Citizen. The Directors have also contributed to the detail.

3.6. A copy of the rules can be provided if requested. Once the Commission has accepted this paper a copy will be published on the Intranet.

Annex 1

The following sets out the main differences that users need to be aware of.

Assembly Members, support staff and police

Old	**New**
Passwords must be changed every 90 days.	Passwords must be changed every 60 days.
No physical restriction on Internet access. Whilst previous rules stated that users should not access certain sites, e.g. webmail, there was no restriction in place and Members and support staff had free access to these sites.	Anything inappropriate / illegal / potentially harmful to the network will be blocked. Access to blocked categories is available via a business case to IT Security. [1] Webmail is not accessible automatically. Users are able to access their Assembly email account via Outlook Web Access (OWA). Blocked categories of website are: Adult/Mature Content; Alternative Sexuality / Spirituality; Chat / Instant Messaging; Email; Extreme; Gambling; Games; Hacking; Illegal Drugs; Illegal / Questionable; Intimate Apparel/ Swimsuits; Nudity; Pay to Surf; Peer to Peer; Personals / Dating; Phishing; Potentially unwanted software; Pornography; Proxy Avoidance; Remote Access Tools; Software Downloads; Spyware Effects / Privacy concerns; Spyware / Malware sources; Suspicious;

	Violence/Hate/Racism; Weapons; Web Advertisements.[2]
USB devices not allowed on any Assembly owned equipment (again this wasn't controlled via a physical policy, but prevented in the rules).	USB ports enabled for use of USB memory sticks. Users need to ensure compliance with information security. Encryption tools available if required. As before, any other USB device can only be connected with approval and after testing.
In addition Members should be aware of changes to personal use of Assembly resources, as set out in the 'Assembly Commission Guidance on the Use of Assembly Resources'. These changes are reflected in the new ICT usage rules.	

Assembly staff and contractors

Old	**New**
Anything inappropriate / illegal / potentially harmful to the network will be blocked. Access to blocked categories is available via a business case to IT Security. Webmail will not be allowed; however, users will now be able to access their work email via Outlook Web Access (OWA)	Anything inappropriate / illegal / potentially harmful to the network will still be blocked and access will still be via a business case to IT Security. Some additional categories that have been opened up in line with External Communications' policy on e-democracy, namely: Social networking sites such as Facebook and video streaming sites such as YouTube.
USB devices not allowed on any Assembly owned equipment.	USB ports enabled for use of USB memory sticks. Users need to ensure compliance with

	information security, in line with data classification. Encryption tools available if required. As before, any other USB device can only be connected with approval and after testing.
No connection to the network is allowed from non-Assembly provided equipment.	OWA is available to staff to enable access to work email accounts via home PCs.

[1] Members who require access to webmail for themselves and/or their staff will need to agree to a short statement that they understand the increased risk to the system caused by such access and to confirm that they believe the access is within the purposes set out in the guidance on the use of Assembly resources. No access for support staff will be granted without the employing Member's permission.

[2] These categories are standard names used by web filter software. A description of each category can be found at annex 2.

Annex 2

Adult/Mature Content

Sites that contain material of adult nature that does not necessarily contain excessive violence, sexual content, or nudity. These sites include very profane or vulgar content and sites that are not appropriate for children.

Alternative Sexuality / Spirituality

Sites that provide information, promote, or cater to alternative sexual expressions in their myriad forms. Includes but is not limited to the full range of non-traditional sexual practices, interests, orientations or fetishes.

This category does not include sites that are sexually gratuitous in nature which would typically fall under the Pornography category, nor does it include lesbian, gay, bi-sexual, transgender or any sites which speak to one's sexual identity.

Sites that promote and provide information on religions such as Wicca, Witchcraft or Satanism. Occult practices, atheistic views, voodoo rituals or any other form of mysticism are represented here. Includes sites that endorse or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, incantations, curses and magic powers. This category includes sites which discuss or deal with paranormal or unexplained events.

Chat / Instant Messaging

Sites that provide chat, text messaging (SMS) or instant messaging capabilities or client downloads.

Email

Sites offering web-based email services, such as online email reading, e-cards, and mailing list services.

Extreme

Sites that are extreme in nature and are not suitable for general consumption. Includes sites that revel and glorify in gore, human or animal suffering, scatological or other aberrant behaviours, perversities or debaucheries. It includes visual or written depictions deemed to be of an unusually horrific nature. These are salacious sites bereft of historical context, educational value or artistic merit created solely to debase, dehumanize or shock. Examples would include necrophilia, cannibalism, scat and amputee fetish sites.

Gambling
Sites where a user can place a bet or participate in a betting pool, participate in a lottery, or receive information, assistance, recommendations, or training in such activities. Does not include sites that sell gambling-related products / machines or sites for offline casinos and hotels, unless they meet one of the above requirements.

Games
Sites that support playing or downloading video games, computer games, or electronic games. Includes sites with information, tips or advice on such games or how to obtain cheat codes. Also includes magazines dedicated to computerized games and sites that support or host online sweepstakes and giveaways.

Hacking
Sites that distribute, promote, or provide hacking tools and / or information which may help gain unauthorised access to computer systems and / or computerised communication systems. Hacking encompasses instructions on illegal or questionable tactics, such as creating viruses, distributing cracked or pirated software, or distributing other protected intellectual property.

Illegal Drugs
Sites that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.

Illegal / Questionable
Sites that advocate or give advice on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism. Also includes sites that provide or sell questionable educational materials, such as term papers.

Intimate Apparel/ Swimsuits
Sites that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. Does not include sites selling undergarments as a subsection of other products offered.

Nudity
Sites containing nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include sites containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist sites that contain pictures of nude individuals.

Pay to Surf
Sites that pay users in the form of cash or prizes, for clicking on or reading specific links, email, or web pages.

Peer to Peer
Sites that distribute software to facilitate the direct exchange of files between users. P2P includes software that enables file search and sharing across a network without dependence on a central server.

Personals / Dating
Sites that promote interpersonal relationships.

Phishing
Sites that are designed to appear as a legitimate bank or retailer with the intent to fraudulently capture sensitive data (i.e. credit card numbers, pin numbers).

Potentially unwanted software
Sites that distribute software that is not malicious but may be unwanted within an organisation such as intrusive adware and hoaxes.

Pornography
Sites that contain sexually explicit material for the purpose of arousing a sexual or prurient interest.

Proxy Avoidance
Sites that provide information on how to bypass proxy server features or gain access to URLs in any way that bypasses the proxy server. This category includes any service which will allow a person to bypass the Blue Coat filtering system, such as anonymous surfing services.

Remote Access Tools
Sites that primarily focus on providing information about and / or methods that enable authorised access to and use of a desktop computer or private network remotely.

Software Downloads
Sites that are dedicated to the electronic download of software packages, whether for payment or at no charge.

Spyware Effects / Privacy concerns
Sites to which spyware (as defined in the Spyware / Malware Sources category) reports its findings or from which it alone downloads

advertisements. It does not contain sites which serve advertisements for other web pages in addition to spyware advertisements; only those sites uniquely used by spyware. Includes sites that contain serious privacy issues, such as "phone home" sites to which software can connect and send user information; and sites to which browser hijackers redirect users. Usually does not include sites that can be marked as Spyware/Malware.

Spyware / Malware sources

Sites which distribute spyware and other malware. Spyware and malware are defined as software that takes control of a computer, modifies computer settings, or collects or reports personal information without the permission of the end user. It also includes software that misrepresents itself by tricking users to install, download, or enter personal information. This includes sites or software that perform driveby downloads; browser hijackers; dialers; software that does intrusive advertising; any program which modifies your browser homepage, bookmarks, or security settings; and keyloggers.
It also includes any software which bundles spyware (as defined above) as part of its offering. Information collected or reported is "personal" if it contains uniquely identifying data, such as email addresses, name, social security number, IP address, etc. A site is not classified as spyware if the user is reasonably notified that the software will perform these actions (e.g. it alerts that it will send personal information, be installed, or that it will log keystrokes).

Suspicious

Sites considered to have suspicious content and / or intent. This categorisation is determined by analysis of web reputation factors. If a site is determined to be clearly malicious or benign, it will be placed in a different category.

Violence / Hate / Racism

Sites that depict extreme physical harm to people or property, or that advocate or provide instructions on how to cause such harm. Also includes sites that advocate, depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other involuntary characteristics.

Weapons

Sites that sell, review, or describe weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications. Does not include sites providing information on BB guns, paintball guns, black powder rifles, target shooting, or bows and arrows, unless the site also meets one of the above requirements. Also does not include sites that promote collecting weapons, or groups that either support or oppose weapons use.

Web Advertisements

Sites that provide online advertisements or banners. Does not include advertising servers which serve adult-oriented advertisements.