POLICY TITLE

Appendix 3G - Wireless Data Communications Policy

1. **Introduction**

This policy describes requirements for access to the Authority's networks via wireless communication mechanisms. This policy also describes the requirements for creation of new wireless networks and the modification of existing wireless networks. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by the Authority are approved for connectivity to the Authority's networks.

2. **Scope**

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, printers, handheld scanners etc.) connected to any of the Authority's internal networks or devices. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to the Authority's networks do not fall under the purview of this policy (i.e. isolated wireless phones, ham radio etc).

3. **Policy**

3.1. **Registration of Access Points and Wireless Network Cards**

All wireless Access Points / Base Stations / Switches must be registered and approved by the Authority. Access Points / Base Stations are subject to periodic penetration tests and audits. Project Co will allow access to the Facility for and cooperate with such tests and audits and will resolve any issues arising from such tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in wireless devices must be registered with the Authority.

3.2. **Wireless Encryption and Authentication**

All computers with wireless LAN devices must utilize an Authority approved wireless encryption connection method (at a minimum WPA/TKIP) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption mechanisms of at least 1024 bits cipher strength. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against a RADIUS service.

3.3. **Setting the SSID**

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier. SSIDs will be configured with beaconing disabled.

4. **Suitability**

For data networks, wireless networks should not be considered a replacement for a wired network. They should be seen only as an extension to the existing wired network for general purpose access in areas of transient use such as common areas, meeting rooms and areas with fluctuating user counts. Wired network access should always be the first option considered for provision of data services.

A wireless access point provides shared bandwidth. As more users connect to the access point, the available bandwidth per user diminishes. Therefore, wireless networks are not appropriate for high bandwidth applications including high quality video streaming or digital imaging. It is most suited for applications such as voice, text based client systems (telnet), email and web browsing.

POLICY TITLE

Appendix 3G - Wireless Data Communications Policy

The Authority may restrict access to wireless technologies that the Authority considers may be disruptive to existing wireless networks or pose a significant risk to the Authority.

5. **Procedure**

5.1. **Requesting access to existing wireless network(s):**

REASON : to control the growth of the number of users thereby maintaining availability of the wireless network for all users

5.1.1. Users requiring wireless access are required to submit a request for access form to the Authority. A request for access must include detail on frequency of use and type of use. Submission of a request does not guarantee approval.

5.1.2. An e-mail confirmation of receipt will be sent upon receipt of a completed form.

5.1.3. If approved, the Authority will provide detail on setup for access to the wireless network

5.1.4. If the addition of a user results in the need for the installation of additional hardware, Project Co will be responsible for the costs associated with the additional hardware

5.2. **Modification to an existing wireless network:**

REASON : to ensure the wireless networks remain consistent in use to avoid changes on-the-fly which may indirectly create security risks or impact availability of wireless services for existing users.

5.2.1. Departments requiring change or expansion of existing wireless networks must provide a minimum of 4 weeks notice of the change requirement to TAS

5.2.2. If the change or expansion creates unacceptable increased risk the request will be denied

5.2.3. Expansion of services requiring resources beyond 8 hours estimated time will require an additional week of lead time, with an additional week for each 20 hours of resources required

5.2.4. Expansion projects will include costs for risk analysis, penetration testing, and associated documentation changes and data entry time where required for MAC address entry and certificate management functions

5.3. **Creation of new wireless networks**

REASON : to ensure new wireless networks are implemented in the most secure way possible and implemented according to policy.

5.3.1. Departments requiring wireless networks are required to submit a project plan in advance of product selection

5.3.2. New wireless networks will be subject to penetration testing and security audits

5.4. **Communicate the intended use of wireless networks**

REASON : to ensure all users are aware of the intended use of a wireless network to avoid creating unnecessary and unintended risk

5.4.1. The intended use of the wireless service will be communicated to the end user to ensure the wireless service is only used for it's intended purpose.

5.4.2. Modifications to the intended use of the wireless networks will be considered a modification to the wireless network itself and will require prior approval as outlined in 7.2 above.

5.4.3. Wireless networks will be deployed in such a fashion as the services available will be as narrowly defined as possible and therefore will not be the same as those available

on the physical wired network. Changes to the intended use may cause issues to be reported erroneously.

6. **Definitions**

Terms	Definitions
User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used
Device Authentication	A method by which a device attempting to connect to the wireless network is authenticated as a legitimate device
Encryption	A method by which data transferred between two entities is deemed illegible by an intercepting body or individual
TAS	The Authority's Technical Architecture and Security Group