Bulletin: Wireless LAN Access Policy

DATE: June 17, 2005

OBJECTIVE

This bulletin defines the circumstances, terms and conditions by which PLNet clients provide wireless connectivity to PLNet.

BACKGROUND

This document attempts to outline the basic requirements and security precautions expected of PLNet customers deploying wireless (802.11) access technology. This establishes standards for access to PLNet with this technology. This policy does not apply to dedicated point-to-point wireless solutions.

GENERAL POLICY

PLNet is part of SPAN/BC. Together they support 2000 educational institutions, 1500 government offices, and 300 other agencies and programs. Security and reliability of the Network is a collective responsibility. No single organization should permit activity that jeopardizes the operations of the Network.

This standard governs the controls that are required when allowing users to connect to the Network wirelessly. This Policy is also recommended for all LAN access regardless of how it is achieved.

EXISTING SERVICES

Where a PLNet client has an existing wireless network, they must ensure that their existing service meets this updated policy, as soon as practical.

STANDARDS

1. A secure location is required for the communications equipment and communications server (e.g. no unauthorized access).
2. Logical Controls for wireless LAN access must include a minimum of three (3) of the following:
   a. Media Access Control (IEEE 802 data link layer) (MAC) address controls
   b. Hidden Service Set IDentifier (SSID)
   c. Wireless Encryption Protocol (WEP) (minimum) or Wi-fi Protected Access (WPA) (preferred) access control
   d. LAN authentication using a robust standard such as Kerberos or RADIUS
   e. Disabling user identifiers after no more than six (6) consecutive unsuccessful password attempts

3. Passwords used shall include common practices to avoid the authentication system being compromised, such as:
    a. pseudo-random in nature or verified by an automated process designed to counter triviality or repetition
    b. of sufficient length to avoid brute-force cracking
    c. changed at least every 40 days
    d. contain a mixture of characters, both upper and lower case, numbers, punctuation, and special symbols
    e. not be a dictionary word
4. Local Administrative policy shall specify those individuals who are authorized to perform security functions for the management of the wireless service, such as resetting passwords, providing security guidance and advice for users.
5. Internal audit procedures, such as all changes being clearly documented, ensure administration functions and help identify security problem sources.

INDEMNITY

Nothing in this document should be taken as a recommendation as to the suitability or security of wireless services. Furthermore, the PLNet client agrees to indemnify PLNet, the Province, its employees and agents against all claims, demands, losses, damages, costs and expenses made against or incurred, suffered, or sustained by the Province arising out of connections provided locally and agrees that in no event will the Province be liable for any damages, including but not limited to any incidental, special or consequential damages, arising out of or in connection with the use or inability to use these services.

The PLNet Helpdesk will not be responsible for fielding trouble calls regarding end users accessing VPN, or wireless LAN access provided locally.

In the event of a security incident, the PLNet Helpdesk will advise the customer as soon as practical. The PLNet site should remove the equipment that is the source of the incident until the problem can be remedied. If there is an immanent security threat, CITS Network Operations has been authorized to block access from the offending IP address or from that entire site depending on the nature of the threat. Such blocking may occur prior to contacting the site.

Responsibility Centre: PLNet

FOR MORE INFORMATION CONTACT: PLNet Help Desk 1-888-769-5678 or send an email to plnetbc@eds.com