Bulletin: PLNet Dial-in Policy

DATE: June 17, 2005

OBJECTIVE

This bulletin defines the circumstances, terms and conditions by which PLNet clients may provide dial services that connect to PLNet.

BACKGROUND

This document attempts to outline the basic requirements and security precautions expected of PLNet customers who deploy remote access technology. This policy establishes standards for dial-in access to PLNet. This document supersedes all previous bulletins on dial-in access.

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.

EXISTING SERVICES

Where PLNet clients have existing dial-in access, they are encouraged to use commercial providers or CITS-provided remote access solutions (SPAN/dial or VPN). Where this is not practical, the PLNet clients must ensure that their existing service meets this updated policy.

PERFORMANCE

PLNet clients will be responsible for managing the utilization of their PLNet connection by dial-in users, to ensure that there are no adverse performance impacts. The costs of any performance improvements required will be borne by the PLNet client

STANDARDS

1. Physical controls for dial-in service must include;
    a. a secure location for the communications equipment and communications server (e.g. no unauthorized access)
    b. protected terminal junction boxes for the inbound telephone trunk lines
    c. surge protectors for the communications equipment
2. Logical controls for dial-in service must include:
    a. a robust user authentication mechanism that uses user-identifiers and passwords, such as Kerberos, NIS+, RADIUS
    b. disabling user identifiers after six (6) unsuccessful password attempts
    c. passwords must be generated, controlled and distributed in a manner that maintains the confidentiality and integrity of the password
    d. usernames and passwords must allow for the unique identification of the end station or end-user, such as no generic accounts, for example

3. Passwords used shall include common practices to avoid the authentication system being compromised including;
    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 dial-in 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

The PLNet client agrees that dial-in access services through PLNet are provided without any warranty as to suitability. 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 these dial-in connections 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 dial-in access provided locally.

In the event of a security incident, the PLNet Helpdesk will advise the customer as soon as practical. The PLNet site will 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