COUNSEL'S CHAMBERS LIMITED

P: +61 2 9231 3644
E: admin@ccl.com.au
W: www.ccl.com.au
A.B.N. 72 000 111 302

Level 1 Selborne Chambers
174 Phillip Street Sydney
NSW 2000 Australia
DX: 973 Sydney

COUNSEL'S CHAMBERS LIMITED POLICY DOCUMENT

Network Interconnection Policy (Data and VoIP)
Date: 06 March 2007
Edition: **1.1**
Source: The Board of Directors of Counsel's Chambers Limited

1.0 Purpose

The purpose of this document is to protect the Counsel's Chambers Data and VOIP Network ("the CCL Network"), and the users of the CCL Network from malicious activity, either passive or active, from the Internet.

2.0 Scope

The scope of this policy is to define the appropriate physical interconnection of IP networks, where one party is part of the CCL Network. This includes both wired wireless networks.

3.0 Rationale

Firewalls protect a network from malicious activity from the Internet by sectioning network hosts into various zones, and permitting or denying traffic between these zones.
Hosts 'inside' the firewall, are trusted, meaning that traffic can flow unhindered between hosts residing in the same zone.
If a host is 'multi-homed', there is thus created a back door, or security hole, into the CCL Network, leaving not only the multi-homed host, but other hosts in the same security zone, exposed to threats from the Internet (particularly, malicious activity).

4.0 Policy

Hosts connected to the CCL Network must not be configured so as to act as a bridge, switch, hub or router between the CCL Network and any other network.

Hosts connected to the CCL Network must not in any way be connected simultaneously to the CCL Network and to any other computer network by means including but not limited to dial-up, DSL, cable or wireless.

Hosts which are used on other networks (such as connecting a notebook computer at home) must maintain and run an up-to-date virus scan before reconnecting to the CCL Network.

Network infrastructure, such as switches and routers, forming part of the CCL Network may not under any circumstances be connected to any other network. The exception to this is CCL Network's connection to its service provider which is a dedicated 10Mbit fibre connection that is logically separated from the Network via a hardware firewall which is configured to be compliant with CCL Network's internal network security policy.

5.0 Enforcement

Any breach of this policy will result in the immediate disconnection from the CCL Network of the offending hardware or bridge without warning or notice, until the interconnection is removed by the owner of the hardware. Any users of the CCL Network found engaging in this activity are liable to be denied further access to the CCL Network without notice.

The cut-off of services is not dependent upon any damage having been caused to the network or any user(s) of it, or infiltration occurring prior to the time of cut-off.
The cut-off is not in lieu of any damages which may be caused to the network or any user(s) and each user specifically absolves Counsel's Chambers Limited from any liability for any cut-off by the CCL Network in the circumstances listed in this section.

6.0 Definitions

Bridge: Device which interconnects networks on OSI Layer 1 or 2 (Open Systems Interconnection Reference Model – an abstract model for networks published by the ISO)
CCL Network: The computer, data and VoIP network including all hosts (computers, switches, hubs, routers, firewalls and other networking hardware) owned or operated by Counsel's Chambers Limited, and all devices connected by a wired or wireless connection to these.

Firewall: Software or hardware that acts as filter of data as it travels through a network.
Host: A piece of computer hardware which is connected to a network. This includes PCs, notebooks, PDAs (Portable Digital Assistants), switches, routers, network printers, servers, wireless access points etc.
IP Network: A network of hosts, communicating on the Internet Protocol.

Malicious Activity: Any activity that compromises or potentially compromises the security, integrity and/or privacy of data residing on or moving through the CCL Network or the CCL Network itself or which denies access to or unreasonably slows the speed of the CCL Network and/or hosts residing on the CCL Network.

Multi-homed host: A host which has more than one network connection.
Network: Computer or data or VOIP network. This includes both wired and wireless networks.
Router: Device which interconnects networks on OSI Layer 3 Switch/Hub: Device which interconnects networks on OSI Layer 2