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

Rev 2.1 08 May 2017

CCL's Wireless Network Connections Policy

PURPOSE

The purpose of this document is for Counsel's Chambers Limited (CCL) to take measures to protect the Counsel's Chambers Data and VoIP Network ("the CCL Network"), and the users of the CCL Network from unauthorised access, malicious activity, either passive or active, from malicious attackers utilising wireless technologies.

SCOPE

The scope of this policy is to define the appropriate use of wireless networking technologies on any part of the CCL Network. This includes technologies such as but not limited to the IEEE 802.11 series of standards.

RATIONALE

The increasing prevalence of wireless technology can create major security holes within the CCL Network, giving unauthorised access to both user systems and networks. Most wireless technologies and devices are insecure by default, and many authentication and authorisation schemes that are widely used provide insufficient, if any, security.

POLICY

Installation

Installation of wireless devices to be connected to or which are able to access the CCL network must be first approved by CCL in writing and all installations maintenance must be performed by a CCL approved contractor. Approval can be granted upon application to Counsel's Chambers Limited. Approval is subject to a written undertaking to comply with this and all other policy documents published by CCL from time to time.

The owner/operator of the device must also sign the form provided by CCL which is attached to this Policy and marked 'A'. By the execution of this form the owner/operator of the device indemnifies CCL and the users of the CCL network against any damage or malicious activity arising from the installation or use of the wireless device.

Wireless access points may only be installed for the use by existing CCL Network users. Encryption keys or credentials must not be provided to third parties, including guest access and existing and new network users.

Minimum Security Requirements

All wireless devices must provide adequate authentication and authorisation of devices connecting to it, and must prevent all unauthorised access.

All data traversing the wireless link must be encrypted such that it is not possible for an unauthorised person or device to decrypt it.

Encryption keys must be changed on a regular basis and must meet minimum strength requirements.

The minimum approved standard for encryption will be revised from time to time.

WPA2 Personal is currently the minimum approved encryption standard.

WPA2 with authentication is the current recommended standard.

Personal Area Network (PAN) devices which use protocols such as Bluetooth and Infrared must use high levels of encryption where available, and should be disabled when not in use.

ENFORCEMENT

Any breach of this policy will result in the immediate disconnection from the CCL Network of the offending hardware without warning or notice. Any users of the CCL Network found in breach of this policy 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.

DEFINITIONS:

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.

Host: A piece of computer hardware which is connected to a network. This includes PCs, notebooks, smartphones, tablets, switches, routers, network printers, servers, wireless access points etc.

IEEE 802.11: The Institute of Electrical and Electronics Engineers, Inc (IEEE) is a global professional association, who develop and publish standards, particularly relating to technology and communications. The 802.11 family of standards defines the specifications for wireless LAN technology.

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.

Network: Computer or data or VOIP network. This includes both wired and wireless networks.

Wireless Device: A piece of computer hardware that communicates with other devices using protocols including but not limited to IEEE802.11 (“Wi-Fi”), Bluetooth and IrDA (infrared).

WEP: Wired Equivalent Privacy, defined in the IEEE 802.11 standards in an attempt to facilitate secure wireless communications. This protocol has serious flaws and does not provide an adequate level of privacy, security, or data integrity

WPA: Wi-Fi Protected Access. This encryption scheme can use an 802.1 lx authentication server, or can use Pre-Shared Keys (“personal” mode). For this scheme to be secure, strong passwords must be used.

WPA2: Defined in IEEE 802.1 li, the currently recommended security standard. If using Pre-Shared Key mode, the password length must be at least 20 characters and not vulnerable to Dictionary Attacks.