COUNSEL'S CHAMBERS LIMITED
POLICY DOCUMENT
Network (Data & VoIP) Connection Terms & Conditions

Date: 5 August 2015

Edition: 2.0

Source: The Board of Directors of Counsel's Chambers Limited

1.0 PURPOSE

The purpose of this document is to outline further terms and conditions on which connection/access is granted to the CCL Network. These further terms and conditions have been developed in order to protect the Data and VOIP component of the CCL Network (the "CCL Data/VOIP Network"), and the users/members of the CCL Network from malicious activity, either passive or active, from the Internet.

2.0 TERMS & CONDITIONS

Network Members and Member Floors agree that access/connection to the CCL Data/VOIP Network is granted on the following terms and conditions;

(a) The terms of CCL's Acceptable Use Policy, the Other Network Policies (as defined in CCL's Acceptable Use Policy) and the Macquarie Telecom Services Agreement Acceptable Use Policy, as amended from time to time, must be complied with;

(b) Virus definitions must be kept up to date and members must run frequent virus scans;

(c) Security patches for software and operating systems must be promptly applied;

(d) Login credentials must not be disclosed to anyone and members acknowledge that account misuse will result in immediate and permanent disconnection;

(e) Attached is a Summary of the Cisco End-of –Life Policy. Hardware connected to the CCL Network must be replaced prior to it being categorised as "end-of-life";

(f) Members acknowledge that hardware connected to the CCL Network that is categorised as being "end-of-life" will be disconnected from the CCL Network;

(g) Only Cisco brand switching devices are permitted to be connected to the CCL Network Core;

(h) Network Members and Member Floors acknowledge that it is the responsibility of individual Floors to replace hardware that has reached "end-of-life." In particular

Member Floors are responsible for the hardware replacement costs of the Floor Cisco Switching devices.

(i) No equipment may be connected to the CCL Network Core without the express permission of CCL;

(j) Member Floors acknowledge that CCL will pay the ongoing annual maintenance costs associated with the individual Floor Cisco Switches (with the exception of those switches located on non-shareholder floors, in this situation, CCL will pay the maintenance costs and CCL will then invoice the floors for this service). Administration access to these Switches is to be exclusively controlled by CCL;

(k) To ensure compliance and security, CCL will pay the annual maintenance costs for the services provided under the banner of the CCL VoIP service, being the software maintenance for the Consoles (switchboards) and the Cisco maintenance for the CUWL and Unity/Cups licences (voicemail & presence). This cost will be invoiced by CCL to Member Floors annually for these services and Member Floors must reimburse CCL within 30 days from the date of the invoice. Failure to reimburse CCL for these maintenance services will result in disconnection from the VoIP service;

(l) Again to ensure compliance and security, Member Floors acknowledge that CCL will pay the cost for major software upgrades that is not covered under the annual software maintenance as described in (k) above. This cost will be invoiced by CCL to Member Floors at the time that the expense is incurred and Member Floors must reimburse CCL within 30 days from the date of the invoice. Failure to reimburse CCL for these upgrades will result in disconnection from the VoIP service. Major version upgrades related to the Arc consoles are described in the attached end-of-life policy document;

(m) Network Members and Member Floors acknowledge that CCL will be responsible for the maintenance contracts for all CCL Network Core equipment and floor access switches directly connected to the CCL Network Core. Network Members and Member Floors are responsible for the maintenance contracts on all other equipment and software connecting to the CCL Network either physically or over wireless access technologies, unless otherwise described in these conditions. In addition to personal computers, this equipment will also include any equipment deployed by Member Floors to facilitate connection to CCL's wireless service.

(n) CCL reserves the right to change or update these terms and conditions and other CCL Network policies without notice. All current terms and conditions and policy documents will be published on the CCL website: www.counselschambers.com.au

Macquarie Telecom Services Agreement
Acceptable Use Policy

This Acceptable Use Policy (**Policy**) sets out certain additional obligations of the Customer under the Agreement. Any capitalised terms not defined in this Acceptable Use Policy have the meaning given to them in the current version of the Macquarie Services Agreement Trading Terms, a copy of which is available at *www.macquarietelecom.com*.

1. GENERAL POLICY STATEMENT

1.1 The Customer must not (and must ensure that any person using the Services (**User**) does not) use or attempt to use the Services or any Macquarie Telecom Equipment, the Macquarie Telecom Backbone, or the equipment or Network of a Provider, in any manner that violates:

(a) any applicable local, state, federal or international law (including, without limitation, the *Spam Act 2003 (Cth)* (**Spam Act**) and the *Copyright Act (1968 (Cth)*); or

(b) the rights of any third party (including, without limitation, infringement of copyright, trademark, or other intellectual property right, misappropriation of trade secrets, electronic fraud, invasion of privacy, pornography, obscenity and libel).

1.2 The Customer must not (and must ensure that any User does not) in the course of using the Services engage or attempt to engage in any activities that:

(a) interfere with or disrupt other Network users, Network services or Network equipment;

(b) involve the unauthorised use of any machine or network, denial of service attacks, falsifying header information or user identification information, monitoring or scanning the networks of others; or

(c) introduce or allow the introduction of any virus, worm, trojan horse, zombie, keylogger or other malicious code into the Services or any Network.

1.3 For the purpose of **clause 1.2**, interference or disruption includes, without limitation, distribution of unsolicited advertising or chain letters, repeated harassment of other Network users, impersonating another such user, falsifying one's network identity for improper or illegal purposes, sending unsolicited bulk emails or calls, continuing to send someone email after being asked to stop, propagation of computer worms and viruses, mail bombing and "flashing" and using a Network to gain unauthorised entry to any other machine accessible via a Network.

2. SPAM

2.1 In this clause, "**spam**" includes one or more unsolicited commercial electronic messages with an Australian link for purposes of the Spam Act, and derivations of the word "**spam**" have corresponding meanings.

2.2 The Customer may not use the Service to:

(a) send, allow to be sent, or assist in the sending of spam;

(b) use or distribute any software designed to harvest email addresses; or

(c) otherwise breach the Spam Act or the *Spam Regulations 2004 (Cth)*.

2.3 Macquarie Telecom may suspend the Services in the following circumstances:

(a) if the Services are being used to host any device or service that allows email to be sent between third parties not under the Customer's authority and control; or

(b) if the Customer or any User is in breach of **clause 2.2**,

provided however that Macquarie Telecom will first make reasonable attempts to contact the Customer and give the Customer the opportunity to address the problem within a reasonable time period (having regard to the severity of the problems being caused by the open service or breach referred to above.

2.4 The Customer must use its reasonable endeavours to secure any device or network within the Customer's control against being used in breach of **clause 2.2** by third parties, including where appropriate:

(a) the installation and maintenance of antivirus software;

(b) the installation and maintenance of firewall software; and

(c) the application of operating system and application software patches and updates.

Macquarie Telecom's right to suspend the Customer's account applies regardless of whether the open service is provided or the breach is committed intentionally, through mis-configuration, or by other means not authorised by the Customer including but not limited to through a Trojan horse or virus.

2.5 In accordance with its responsibilities under the Spam Act and the Internet Industry Association Spam Code (**Spam Code**), Macquarie Telecom may:

(a) restrict the Customer's ability to forward emails;

(b) limit the Customer's access to the Service to a closed user group relevant to its use of the Service;

(c) scan Macquarie Telecom allocated IP address ranges to detect open or otherwise misconfigured mail and proxy servers and suspend the Service if the Customer fails to rectify any problem found within a reasonable period following receipt of a notice from Macquarie Telecom; and

(d) require the Customer to take all necessary actions to comply with, or which assist Macquarie Telecom to comply with, the Spam Act or the Spam Code.

3. CONTENT PUBLISHING

3.1 The Customer must not publish material that is or would be classified by the Classification Board as RC or X rated via websites, email, newsgroups or other publishing mediums accessible via the Services.

3.2 The Customer must take appropriate precautions to prevent minors from accessing or receiving any content the Customer has published that may be inappropriate for them. This includes implementing a restricted access system on content that is or would be classified by the Classification Board as R rated.

4. CUSTOMER EQUIPMENT

4.1 The Customer is responsible for ensuring in relation to any Customer Equipment that:

(a) the Customer Equipment complies with any applicable ACMA code or other applicable specification required for safe and proper use;

(b) use of the Customer Equipment will not infringe any law or third party rights (including without limit any intellectual property rights);

(c) the Customer Equipment is operated by operators familiar with the Customer Equipment and instruction manuals and in accordance with published specifications and manufacturers' guidelines; and

(d) the operating environment conforms to the published specifications and requirements of the Customer Equipment, including stable, spike-free electricity supply, air conditioning, service clearances, cable runs, and complies with any relevant occupational health and safety requirements.

Macquarie Telecom Services Agreement
ACCEPTABLE USE POLICY

4.2 Subject to compliance with the Customer's usual security and access arrangements (if applicable and absent any Emergency), the Customer will provide Macquarie Telecom and any of its authorised representatives with full, free and safe access to the Customer Equipment and any Macquarie Telecom Equipment or any property owned by another Provider located at the Customer's Premises or any other location under the direction or control of the Customer, to the extent required to enable Macquarie Telecom or any Provider to provide the Services.

5. ACCESS AND USE OF FACILITIES

5.1 If the Customer or any of its personnel, agents or representatives access or use any land, site, facilities, equipment, hardware or software of Macquarie Telecom, those parties must comply with all:

(a) applicable laws, regulations, codes and standards that apply to such access or use;

(b) Macquarie Telecom policies, manuals and procedures that apply to such access or use (as may be amended by Macquarie Telecom from time to time) including all operational, induction, security and work, health and safety policies; and

(c) directions of Macquarie Telecom made from time to time in connection with such access or use.

6. BREACH OF THIS POLICY

6.1 If the Customer or any User uses the Service in a way that Macquarie Telecom, in its absolute discretion, believes breaches this Policy, Macquarie Telecom may take any action it deems appropriate to respond to such a breach.

6.2 Actions that Macquarie Telecom may take pursuant to **clause 6.1** include (but are not limited to):

(a) temporary or permanent removal of content and content publishing capabilities;

(b) filtering of Internet transmissions;

(c) immediate suspension or termination of all or any part of the Service;

(d) if applicable, immediate restriction or denial of access to any land, site, facilities, equipment, hardware or software of Macquarie Telecom;

(e) gather information from the Users involved and the complaining party, if any, and examine transmissions and material on its servers and any Network;

(f) cooperate with law enforcement authorities in the investigation of suspected criminal violations and the system administrators at Providers or any other service provider.

6.3 Macquarie Telecom may by notice to the Customer elect to give the Customer 24 hours (or such longer period specified in the notice) to remedy any breach of this Policy, before taking any action pursuant to **clause 6.2**.

6.4 Macquarie Telecom is not obligated to monitor the Customer's or any User's use of the Services (including any content posted, disseminated or accessed by the Customer or any User), but reserves the right to do so to:

(a) identify any breach of this Policy;

(b) enforce this Policy;

(c) protect any other Network users, Network services or Network equipment; and

(d) cooperate with law enforcement authorities in the investigation of suspected criminal violations and the system administrators at Providers or any other service provider. Such cooperation may include Macquarie Telecom providing the username, IP address or other identifying information about a User.

6.5 Macquarie Telecom reserves the right to charge the Customer, on a time and materials basis, for any costs (including labor costs) incurred by Macquarie Telecom as a result of or arising from any breach of this Policy by the Customer or any User. The Customer is liable for any charges invoiced in accordance with this clause.

7. AMENDMENT

This Policy may be amended by Macquarie Telecom at any time without notice to the Customer. The Customer must comply with the terms of the Policy as amended. The current version of this Policy is as posted at *www.macquarietelecom.com*.

Summary of Cisco End-of-Life policy

For hardware products, Cisco follows the following procedure.
Six months before a product is categorised as “End of Sale” a notice is dispatched and the product is listed on the End of Sale web page.
Once the product has reached the End of Sale, it is no longer available for sale through the Cisco point of sale mechanisms.
For the following year new support contracts can be purchased for the product and Cisco continue to provide maintenance releases, bug fixes and critical patches.
For the subsequent four years Cisco may still release software patches, but it may be necessary to upgrade to a different software release. Existing contracts can be renewed but new contracts can not be purchased.
After 5 years from the end of sale date, the product is deemed end of life. Cisco will no longer provide technical support or maintenance releases for the product.

Version upgrades for Arc

Minor version and maintenance releases (eg version 4.5 to 4.6) for the Arc console are included in the annual maintenance fee. Major version releases (eg version 4.x to 5.x) are not covered by the maintenance agreement and attract a per-console upgrade charge which must be done site-wide. Major versions are released every 1.5 - 2 years. Old major versions are only supported for 3 - 4 years after the release of the new version.

References

End of Life policy:
http://www.cisco.com/en/US/products/products_end-of-life_policy.html
End of Sale products:
http://www.cisco.com/en/US/products/prod_end_of_life.html