GRN Acceptable Use Policy

March 2015

Contents

1. Background and Purpose

1.1 This NSW Government Radio Network Acceptable Use Policy (Policy) sets out the rules for NSW Government agencies, partners and third parties (GRN Clients) regarding the use of the NSW Government Radio Network (GRN).

1.2 A GRN Client's right to use the GRN is granted in accordance with the Service Agreement (Agreement) entered into by the GRN Client and the NSW Telco Authority (TA). Any terms used as defined terms in this Policy not defined in this Policy have the meaning given to them in the Agreement.

1.3 The objective of this Policy is to:

(a) Provide details relating to the responsibilities of GRN Clients, as well as highlighting the permitted and prohibited uses of the GRN; and

(b) Ensure that GRN Clients using the GRN do not hinder its operation, interfere with the ability of other users to access and use the GRN, disrupt the business and operations of TA or break any laws.

2. Application

2.1 The Policy applies to all GRN Clients and their employees, agents, officers, contractors and service providers using the GRN in accordance with the Agreement (Authorised Users).

2.2 It is each GRN Client's responsibility to ensure that all of its Authorised Users comply with this Policy.

2.3 Failure of a GRN Client or its Authorised Users to comply with this policy may lead to the suspension or termination of the GRN Client's right to access and use the GRN, together with any other rights or remedies of TA set out in the Agreement.

3. Responsible GRN Use

3.1 In using the GRN and exercising their rights under the Agreement, GRN Clients must ensure that their Authorised Users act responsibly with all reasonable care, prudence and foresight, and with due regard for the rights of other GRN Clients.

3.2 If a GRN Client or its Authorised Users act recklessly, irresponsibly or otherwise in breach of this Policy, the integrity or security of the GRN, or the rights of other GRN Clients, may be threatened or detrimentally impacted. The TA may take any action it believes appropriate, in accordance with the Agreement, to mitigate that threat or impact.

3.3 It is a GRN Client's responsibility to review this Policy regularly, and ensure that all Authorised Users familiarise themselves with its content and understand the potential consequences of a failure to comply.

3.4 If a GRN Client becomes aware of a violation of this Policy by it or its Authorised Users, or by another GRN Client or its Authorised Users, then it must inform the Network Manager as soon as reasonably practicable. The Network Manager's contact details are as advised on the TA website.

4. General Obligations and Prohibitions

4.1 GRN Clients must ensure that their Authorised Users:

(a) not do anything, acting reasonably given the circumstances, which will, or is reasonably likely to, detrimentally impact the ability of other GRN Clients to use or access the GRN;

(b) comply with all standards and NSW Government policies which may be relevant to the GRN as published on the TA website www.telco.nsw.gov.au from time to time;

(c) not disclose to any third party details of the topology or configuration of the GRN, such details being Confidential Information purposes of the Agreement;

(d) not use information relating to the GRN disclosed by or on behalf of TA for anything other than its intended purpose, being the provision of voice and data services on the GRN;

(e) not expose the GRN to cyber security risks through a failure to comply with the Agreement or this Policy, or failing to take reasonable care and attention;

(f) comply with any authorised direction from the GRN's Network Operations and Control Centre (NOCC);

(g) notify the NOCC of any matter relating to their use of the GRN, including:

(i) changes to coverage or loss of TA equipment such as radios;

(ii) planned events and major incidents; and

(iii) other major changes that would impact TA's ability to deliver the GRN services under the Agreement.

4.2 In relation to Customer Support provided to GRN Clients under the Agreement, GRN Clients must, and must ensure that their Authorised Users:

(a) only place customer support calls to the NOCC which relate to the Services and any issues or problems the Client or a User is having in using or accessing the Services;

(b) not intentionally withhold information relevant to the problem from the Network Manager, ; and

(c) direct all support calls or queries to the NOCC in the first instance, rather than to TA, to ensure that all calls can be appropriately tracked and prioritised.

5. GRN Service-specific Obligations and Prohibitions

Trunked Network Access

5.1 Where the GRN Client is receiving Trunked Network Access and has an agreed talk plan under the Agreement, the following are prohibited activities and the GRN Client must not, conduct such activities as:

(a) connecting unapproved devices to the GRN;

(b) creating talk groups in excess of the GRN Client's talk group plan as agreed between the Client and TA (or the Network Manager);

(c) using Talkgroups in a manner that does not comply with the agreed Client Operational Talkgroup Plan, where such a plan exists;

(d) using handsets for other than their intended purpose without TA's authorisation. For example:

(i) using four wire interfaces on radios in an unapproved manner;

(ii) using radio over IP - eg. creating an extension of GRN voice circuits over any networks outside of the TA's administrative control (Untrusted Networks);

(e) connecting radios or other GRN endpoints to Untrusted Networks;

(f) using ESO liaison Talkgroups for purposes other than for ESO liaison.

(g) failing to comply with all applicable rules relating to handset configuration, including:

(i) not adhering to any code-plug standard which applies from time to time;

(ii) implementing other GRN Clients' Talkgroups in radios (without their or TA's permission); or

(iii) duplicating handset configuration (as each radio must have a unique id and alias).

(h) using the emergency button for purposes other than emergency response (such as using it to access the GRN for priority in circumstances where this is unnecessary); and

(i) using handsets for non-work or other unapproved purposes.

Console Network Access

5.2 Where the GRN Client is receiving Console Network Access under the Agreement, the following are prohibited activities and the GRN Client must not conduct such activities:

(a) using Consoles for non-work or unapproved purposes;

(b) using non-approved devices as published on the TA website www.telco.nsw.gov.au;

(c) using backhaul that is not secure (i.e. untrusted or semi-trusted backhaul);

(d) not keeping Consoles under maintenance or using out of date software and/or firmware patched to the manufacturer's recommendation;

(e) failing to ensure that all endpoints have software that detects, prevents and seeks to remove harmful code (being any computer code that is intended or known to be harmful, destructive, disabling or which enables theft, alteration, denial of service, unauthorised disclosure or destruction or corruption of data including viruses, worms, spyware, adware, key-loggers, Trojans), it is the users responsibility to install and maintain industry standard anti-virus software;

(f) failing to have a personal firewall or other software or hardware system that prevents unauthorised access to the GRN Client's private network;

(g) failing to ensure that only appropriately trained users have access to Consoles and they are aware of the potential impact of misuse on the GRN;

(h) connecting Consoles, conventional channel gateways or any other equivalent equipment or devices to any other network or audio source without TA's authorisation; and

(i) connecting Consoles that are not on the approved devices list published on the TA website www.telco.nsw.gov.au.

Customer Enterprise Network (CEN) Access

5.3 Where the GRN Client is receiving Customer Enterprise Network Access under the Agreement, the following are prohibited activities and the GRN Client must not, and must ensure its Authorised Users do not, conduct such activities:

(a) using or obtaining CEN Access without TA's approval. To avoid doubt, approval is required from the Network Manager and the TA Network Services & Operations Manager;

(b) failing to provide a threat risk assessment with an application for CEN Access if requested by TA;

(c) failing to ensure that applications within the CEN are on servers which are patched according to the manufacturer's recommendations, or failing to maintain those applications;

(d) failing to comply to any TA or Network Manager request for details on servers or applications within the CEN for the purpose of network management;

(e) failing to notify TA of any intended use of the CEN, including a list of proposed applications, or failing to communicate any changes to that list;

(f) failing to ensure that applications must be narrow-band and used for machine-to-machine (M2M) or public safety purposes only, and carry mission-critical data only;

(g) using CEN Access for:

(i) high bandwidth applications (a high bandwidth application is one which requires bandwidth to an end user of greater than 9.6 kilobytes per second);

(ii) mobile computing purposes;

(iii) administrative purposes; or

(iv) real-time data transfer or streaming services; and

(h) failing to configure applications to take in to account the technology and capacity of the GRN, such that it does not impact the performance of the GRN for other GRN Clients.

Conventional Network Integration

5.4 In relation to any request for, or provision of, Conventional Network Integration under the Agreement, the GRN Client acknowledges that:

(a) Conventional Network Integration is subject to TA approval on a case by case basis;

(b) Conventional Network Integration is for the extension of conventional radio sites for the purposes of access from GRN handsets and Consoles only;

(c) the connection of other audio sources is not permitted without TA approval; and

(d) cyber security issues are the same as those for Consoles and CENs and the same care must be taken by the GRN Client in respect of those issues.

Handset Rental

5.5 In relation to any provision of handset rental under the Agreement, the GRN Client acknowledges that handsets are to be used for business purposes only, by the relevant GRN Client or its personnel, and handsets are not transferable and must not be provided to any third party without the approval of the TA.

END of DOCUMENT