Third party access to the Secure Digital Radio Network (SDRN)

Table of Contents

The SDRN allows Police to operate and communicate collaboratively and securely with other agencies such as the NZTA FENZ and Customs especially in the case of emergency and disaster Access by anyone outside Police can increase the risk to operational security

This section outlines the process to allow third-party access to the SDRN, and how the risks associated are managed.

Approvals process (for access by third party)

When a third party seeks access to the SDRN, a business case is prepared by them and submitted, via the Director: Emergency Communications Centres and the Chief Information Security Officer (CISO). The business case should include the strategic drivers; risks and opportunities; financial implications and security details at the site(s).

The Director and the CISO will consider the business case before making a recommendation to the Operational Advisory Committee (OAC) and the SDRN Business Owner, Assistant Commissioner: Frontline Capability.

Security agreement

An agreement will be established between Police and the third-party. The agreement should be contained in a schedule to an existing or new MOU or LOA, covering:

- permitted use
- vetting of users
- permitted users/access
- security of information and equipment
- equipment maintenance
- relationship management include dispute resolution
- each organisation's relationship managers
- agreement cancellation clause and equipment removal.

Provision of SDRN equipment is subject to the following conditions:

- the third party meets current costs for the equipment and installation of the sets into the secure operational environment
- ownership of the SDRN base sets remains with Police at all times, as is the right to inactivate and/or remove the equipment and fittings at any time
- maintenance and modification of the equipment must only be carried out by Police
- the third party must provide access for Police to their sites for the installation, maintenance and upgrading of the SDRN equipment
- the third party will notify the Police ICT Service Desk s.6(a) OIA as soon as practicable if any faults arise with the SDRN equipment.

The SDRN equipment and information collected via the network must be protected, including:

- keeping the SDRN equipment within a secure site, with restricted entry
- when there are no staff working in the secure site, that it is alarmed and monitored
- as far as practicable, personal cell phones are left outside and/or headsets are used to prevent others hearing the SDRN traffic
- all staff within the secure site are Police vetted, trained in the use of the SDRN and operate under a confidentiality agreement.

Relationship management

The Director: Emergency Communications Centres is the Police national liaison officer with all SDRN third parties. He or she will manage any issues arising from the installation, use or security of the SDRN equipment.

Each third party also needs to nominate a liaison officer who has oversight of the employees and operations within the SDRN environment. He or she is also responsible for reporting any security breaches.

Printed on : 30/05/2022