Manitoba
Central Services
Public Safety Communications Service

Lost, Stolen or Compromised Radio (Inhibit)

Date Created:	January 10, 2020
Last Updated:	May 13, 2021

Background

To protect the integrity of PSCS, Public Safety Entities (PSEs) are expected to provide continuous accountability and protection against loss or unauthorized access of their radio inventory at all times. Hence, when radios are lost, stolen or compromised it has to be reported immediately to Bell.

Purpose and Scope

To establish and implement a consistent process for reporting a lost, stolen or compromised radio.

Process Input

The process is prompted by the PSE/user reporting a lost, stolen or compromised radio.

It is strongly recommended that PSEs follow the Radio Inhibit process to ensure unauthorized individuals are not able to overhear, or listen in to confidential communications from radios that have been lost, stolen, or provided to a third party for service or repair. PSEs that do not follow the Radio Inhibit process when radio equipment is no longer within their control, assume all risks related to breaches of confidential communications overheard by external parties or individuals.

Process Flow

1. PSE immediately reports lost or stolen radio to his/her Supervisor or Manager.

2. PSE Radio Operator submits a service request via email to BMRadioCC@bell.ca and when possible a follow-up phone call to the Bell Service Desk (1-833-551-3925)-requesting the inhibiting of the radio. In the event that the Operator is not able to send an email at such time, the service desk will request their email to which the case would be submitted. The Bell Service Desk will request the following information:
    a. First and Last name of Requestor along with email address
    b. Radio serial number #, or
    c. Tag number #, and/or
    d. LID number #.

*A *risk has been identified by Bell that an invalid request to inhibit a radio could be provided/requested to Bell in which case a radio could be inhibited from the network causing lost communications to an active radio on the network.*

3. Bell Service Desk will create a case and provide the case number to the PSE. The Service Desk will capture the timestamp of the email or time of phone call as start time of the Service Request. (Service Desk will ensure a copy of the email either received or issued is included as an attachment as part of the case).
4. Bell Service Desk notifies RKA (RCMP KMF Administrator).
5. Bell Service Desk creates a task to the RCAP (Radio Codeplug and Provisioning) team in order to have the radio inhibited from the network.
6. Service Desk will phone the RCAP team in order to ensure that the request has been received, and is being treated with the highest level of priority.
7. RKA determines if the breach has an immediate or future detrimental impact to communications security.
8. RKA advises Bell, on the above, and takes internal corrective action on the KMF.
9. RKA confirms to Bell Service Desk when applicable that encryption keys have been deactivated from the network and radio has been assigned to a different profile.
10. RCAP completes the radio inhibit and informs Bell Service Desk. Prior to the inhibit being performed, a validation of last time the radio was activated on the network will be captured and included in the notes.
11. Service Desk updates the equipment record with the radio updated to a lost state.
12. Bell Service Desk notifies the PSE via email response confirming that the radio has been inhibited.
13. Bell Service Desk closes the case providing a timestamp as to completion. This will allow monthly reporting capabilities on meeting the 2hrs time limit to having radio inhibits completed.
14. Bell recommends that each PSE follow the inhibit process when a vehicle is being brought in for servicing.

Version History

Version	Date	Author	Change Description
1.0		Bell	Initial Release
1.02		Manitoba	Minor Edits
1.03	May 14, 2021	Bell	Bell contact updated