ADMINISTRATIVE PROCEDURE

F1:4
Communication – Communications Systems
Security Incident Management

1. Purpose

This procedure outlines the steps to follow in the event of a security incident, or suspected security incident.

2. Definition of security incident

A security incident may include, but is not limited to the following:

- Loss or theft of a laptop, cell phone, tablet, or external storage device
- Virus outbreak
- Illegal content being accessed, stored, or distributed
- Denial of service attack
- Hacking activities
- Ransomware infection

3. Procedure

Anyone that suspects a security incident has occurred or is occurring must report the incident to ICT Support by calling 1-800-443-4562 and press 1 to speak with ICT support as soon as possible.

All reports of security incidents will be reported immediately to the incident management team.

The incident management team includes the following individuals:

Chief Information Office
Associate Chief Information Officer
Supervisors of ICT

4. Incident Response

Incident response team will discuss the situation based on criteria below and determine an appropriate response.

a) Is the incident actual or perceived?
b) What kind of incident is it?
c) Is the incident still occurring?
d) Is there a data loss?
e) What systems are affected?
f) What is the impact to the network and users?
g) Is the source of the incident internal or external?
h) Do external agencies need to be notified?
i) Do law enforcement agencies need to be contacted?
j) Do additional communications need to occur?

5. Post incident review

Incident response team will review the incident to develop a report based on the following.

a) What was the incident?

b) How did it happen?
c) Were all protective measures in place and up to date?
If no, what was missing?
d) Could it have been prevented?
If yes, how?

6. Recommendations

Incident response team will list recommendations on the following.

a) Were the response steps taken adequate?
b) What is needed to prevent further similar incidents from occurring?
c) What additional steps or procedures are necessary to aid in the response?