Office of the
Saskatchewan Information
and Privacy Commissioner

HUMAN RESOURCE POLICY

2.0 IPC EXPECTATIONS
2.09 MOBILE DEVICE AND REMOTE WORK SECURITY

Purpose
To mitigate risks associated with the use of mobile devices and remote working.

Application
This policy applies to all IPC employees.

Scope
This policy applies to all IPC owned or operated information systems, intellectual property, and IPC records.

Policy
IPC employees must ensure that Mobile Devices in their care:

- Are authorized to use;
- Are only accessed by those authorized to do so;
- Are password protected;
- Are not left unattended;
- Are protected from loss, theft, damage and unauthorized access;
- Has only software authorized for use on the IPC network is installed;
- Has software installed only by those authorized to do so;
- Ensures that sensitive information is not accessed while using mobile devices (i.e. coffee shop, airport, park);
- Ensure the security of home wired and wireless networks if remote working;
- Immediately report the loss or theft of a mobile device to the user's supervisor and the Manager of Administration.

Mandatory Controls for IPC employees are:

- Sensitive IPC information in hardcopy format cannot be stored at a teleworking site unless it is stored in a locked cabinet
- Only IPC issued computers can be used for the processing of IPC information;
- No personal device can be added to the employee's laptop or the network.
- Only approved remote access methods can be used to access the IPC network;
- Patches and updates must be applied when required;
- A home wireless network used to access the IPC network must be secured.

Compliance and disciplinary action

In cases where it is determined that a breach or violation of IPC policies has occurred, the Commissioner will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, or in the case of contractors, vendors, or agents, the termination of a contract or agreement with the contractor, vendor, or agent.

Exceptions

In certain circumstances, exceptions to this policy may be allowed based on demonstrated business need. Exceptions to this policy must be formally documented and approved by the Commissioner.

Authority

The Freedom of Information and Protection of Privacy Act, section 43.1

Influencing Source

Information Technology Resources Policy #2.04
Remote Work Policy #3.06
Use of Office Issued IPhones #3.10