Wireless Networking Security Policy

Last revised: December 2018
Last reviewed: December 2018
Next review: December 2019

Information Security Branch, Ministry of Central Services

This document outlines the Government of Saskatchewan security policy pertaining to Wireless Networking.

Purpose

With the mass adoption of mobile devices, wireless connectivity has become much more commonplace. The Government of Saskatchewan (GoS) network infrastructure is a centrally managed and shared resource. As such, consideration must be made for the capacity, availability and security. Insecure wireless networking can provide an easy attack vector for malicious threat actors.

Scope

This policy applies to all wireless infrastructure devices that *directly* connect to the GoS network or reside on a GoS site that provide wireless connectivity to endpoint devices. This includes any form of directly connected wireless communication device capable of transmitting packet data.

Policy Statements

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to the GoS network. Only those wireless infrastructure devices that meet the requirements specified in this policy or are granted an exception by the Information Security Branch are approved for connectivity to the network.

Authorization

Wireless networks must be authorized by Information Technology Division (ITD).

Individuals and ministries must not independently deploy access points. ITD will work with any ministry wishing to establish or expand WLAN networking in their area.

Security Configuration and Support

Wireless networks must:

- abide by the standards specified by the ITD;
- be installed, supported and maintained by an approved support team;
- use ITD approved user and device network access protocols and government authentication services;
- use Information Security Branch (ISB) approved encryption protocols and key configuration.

Non-interference

Wireless networks must not interfere with wireless access deployments maintained by other support organizations.

Revoking Access

ITD reserves the right to revoke wireless service authorization for any individual device or user.

Compliance and disciplinary action

In cases where it is determined that a breach or violation of GoS policies has occurred, the Information Security Branch, under the direction of the Chief Information Officer and the respective Ministry, 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 Chief Information Officer, under the guidance of the Information Security Office. Policy exceptions will be reviewed on a periodic basis for appropriateness.