Government of Alberta

GoA Domain Network Access Control

Policy Advisory Guide

December11, 2018

Corporate Information Security Office
Service Modernization
Service Alberta

Government of Alberta

Table of Contents

1 Version History

Date	Author	Version	Description of Change
March 2017	Kenneth Lummis	1.1	Updated email addresses and responsibilities
February 2017	Kenneth Lummis	1.2	Update responsibilities and logo
December 18, 2018	Kenneth Lummis	1.3	Update responsibilities

2 Executive Summary

Network Access Control ensures that only authorized devices have access to GoA network services. This Policy Advisory Guide outlines categories of authorized devices that may be provided access to GoA network resources, processes for requesting exceptions for access and provisions for guest access services.

3 Background

The Corporate Information Security Office (CISO) in Service Alberta provides IT security guidance, monitoring, incident management and forensic services.

3.1 Policy Context

Information Security Management Directive 6.8 states that only GoA managed devices shall be connected to internal GoA networks and connected devices must be continuously monitored.

Techniques include user and device authentication prior to issuing network addresses and scanning for unauthorized network equipment.

This guide sets the requirements to implement this control. This guide may be complemented by processes documented and used internally by the CISO and operational teams.

4 Scope of Policy Advisory Guide

Requirements set in this guide apply to the all Ministries and clients connecting to the GOA Domain infrastructure using a GoA Zone 4 network connection.

5 Definitions

- **GOA Domain Managed Device:** a device that is accepted, monitored and maintained by Service Alberta's Service Modernization Division. These devices are generally described in the GoA Service Catalogue.

- **Approved Exception Device:** a device sponsored by a Ministry, has been risk assessed, passed through the exception process, and approved by the CISO as acceptable to connect to a GoA network.

- **Guest Access Device:** a device that is not a GoA Domain Managed Device or an Approved Exception Device. Users may connect a Guest Access Device to a GoA network connection and receive access to the public Internet. No access to GoA internal network services will be available.

- **GoA Network Services:** any service provided by the GoA to enable a device to connect to another device on the GoA network or public Internet.

- **GoA Zone 4 Network:** the internal network managed by Service Alberta's Service Modernization Division.

6 Authorized Devices

All Authorized Devices, except where not possible, must display the following notice to users upon logon when accessing GoA Network Services:

This private network is the property of the Province of Alberta and all usage may be monitored. Approved users accessing this network will do so in accordance with existing policies and the Alberta Public Service values.

6.1 GoA Managed Devices

GoA Managed Devices will be provided the minimum access required to GoA network services required to meet service requirements. Examples of GoA Managed Devices include:

- GoA Workstations and Laptops
- SecureNet Wireless Access Points
- Managed Network Printers
- Managed Uninterrupted Power Supplies (UPS)
- Voice-over-IP (VOIP) Phones

GoA Managed Devices may be subject to an automated security assessment, quarantine and if required remediation for security weaknesses, prior to being granted access to all GoA network services.

6.2 Approved Exception Devices

Sector Chief Information Officers may request that devices not managed by Service Modernization be granted an exception to access GoA network services. Exceptions will be granted for up to one year and may be renewed by submitting a new request.

The intention of this provision is to provide consideration for Ministry or for third party owned devices that cannot be adequately accommodated through the Guest Portal.

A service request to request Network Access Control Exception for a device must include:

- Description of device
- Person or business unit responsible for maintaining the device
- Business justification for the exception
- MAC Address
- A commitment to manage security vulnerabilities including to apply all vendor recommended security patches
- Requested level of access (e.g. required GoA network services or Internet access)
- Endorsement from Ministry CIO

The CISO will review all service requests for Network Access Control Exceptions and render a decision based on risk factors to the GoA.

6.3 Guest Access Devices

Devices that are not recognized as GoA Domain Managed Devices or Approved Exception Devices will not be granted access to internal GoA Network Services. These devices will be routed directly to the internet.

7 Roles and Responsibilities

7.1 Device Classification Project Team

The project team is responsible for initial setup and configuration of Network Access Control.

- Enable all GoA Zone 4 network locations with Network Access Control capability
- Identify GoA Managed Devices at all sites
- Assist Ministries in identifying non-GoA Managed Devices advise Ministry of options

7.2 Service Alberta Infrastructure Operations (IO)

Upon closure of the Device Classification Project, Network Access Control will be integrated into normal GoA network operations in IO. IO will be responsible for managing and maintaining the Network Access Control system including responding to incidents where devices cannot connect to GoA Network Services.

7.3 Sector Chief Information Officers (CIO)

Sector CIOs are responsible identifying potential exception requests and submitting as required to the CISO. This will occur in ITSM through the Infrastructure Request Coordinator (IRC).

7.4 Service Alberta ICT Service Delivery and Support

Service Alberta Client Relationship Management is responsible for providing service request processes to request changes to Network Access Control services including submitting and processing Network Access Control Exception Requests.

7.5 Corporate Information Security Office (CISO)

The CISO is responsible for

- Reviewing and making a decision on exception requests
- Monitoring GoA network services for potential vulnerabilities or security threats and taking action
- Developing security policy instruments

8 Contact List

8.1 Corporate Information Security Office

8.1.1 Management Contacts

For questions about this Policy Advisory Guide, please contact:
Kenneth Lummis
Manager
kenneth.lummis@gov.ab.ca
ciso@gov.ab.ca

9 References

1. Information Security Management Directives