ACCEPTABLE USE OF MOBILE DEVICES POLICY

POLICY STATEMENT

This policy establishes the following guidelines, procedures and processes for the acceptable use of mobile devices by the user with respect to the following:

- Using mobile devices to carry out Government of Nunavut (GN) and/or personal business;
- Connecting to the Government of Nunavut's network, software or data using a mobile device;
- Ensuring information exchanged or decisions made on mobile devices is properly recorded, documented, stored and managed according to all applicable acts and policies;
- Ensuring the security and integrity of information accessed or contained on mobile devices;

PRINCIPLES

This policy is based on the following principles:

- The GN provides handheld wireless devices to employees where it is necessary for the effective performance of an employee's duties. These services shall only be used in a manner which protects system resources and the information stored therein, and is accountable and consistent with the provision of ethical, courteous and professional service to Nunavummiut and all related records management and access to information acts and policies.

- The GN has an obligation to protect government information and to maintain the continuity of government services.

- The GN is committed to Inuit Qaujimajatuqangit principles of *Piliriqatigiinniq-Ikajuqtigiinniq* (working together for a common cause), *Pilimmaksarniq-Pijariuqsarniq* (development of skills through practice, effort and action) and *Qanuqtuurniq* (being innovative and resourceful).

- The GN has an obligation to protect personal information by making reasonable security arrangements against unauthorized access, collection, use, disclosure or disposal of information and records under its control.

APPLICATION

This policy applies to all GN employees, contracted resources and any additional users that use mobile devices to access, store, back up, or relocate any Government of Nunavut or client-specific data.

Such access to this confidential data is a privilege, not a right, and forms the basis of the trust the GN has built with its clients, supply chain partners, and other constituents.

Employment or contractual services with the GN does not automatically guarantee the initial or ongoing ability to use these devices to gain access to government networks and information.

This mobile device policy applies, but is not limited to, all devices and accompanying media that fit the following classifications:

- Smartphones
- iPads
- Mobile/cellular phones
- Tablets
- E-readers
- Portable media devices
- Laptop/notebook computers
- Wearable computing devices
- Any other mobile device capable of storing data and connecting to a network

In order to maintain security and manageability, the policy applies to any mobile hardware that is used to access government resources.

Any GN or client information, network or data accessed on a personal mobile device is subject to same acceptable use and records management provisions outlined in this policy.

DEFINITIONS

- **"Mobile devices"** includes: Smartphones, iPads, mobile or cellular phones, tablets, e-readers, portable media devices, laptop/notebook computers, wearable computing devices and any other mobile device capable of storing data and connecting to a network;

- **"Employee"** refers to an individual employed by the Government of Nunavut and its crown corporations or agencies, including individuals retained under contract to perform services for the GN;

- **"User"** refers to an employee, contractor, student or individual using GN network services or devices.

- **"Information"** includes any data, record, report, e-mail or other information accessed through Government of Nunavut networks, or created or exchanged on mobile devices as part of a discussion related to GN business.

- **"Network"** includes any Government of Nunavut telecommunications system, network or program administered by the GN, including e-mail, shared drives and folders, remote access programs, or other media.

DIRECTIVES

1. **Records Management**

a. The *Archives Act*, the *Access to Information and Protection of Privacy Act*, *Records Management Act* and other related policies and information security procedures require that information, actions and decisions taken by Nunavut public servants be properly recorded, documented and secured, thus creating a government record.

2. **Procurement and Connectivity**

a. Departments must provide CGS Informatics and Planning Services (CGS-IPS) with specific device requirements and specifications prior to purchasing devices that are to be directly connected to the GN network. CGS-IPS has to pre-approve devices prior to purchase and connection to the network. Once received, for devices that will be directly connected to the GN network, CGS-IPS will manage all aspects of device configuration and installation related to the security of their device.

b. Connectivity of all mobile devices on the core GN network will be centrally managed by CGS-IPS and will use authentication and appropriate encryption measures wherever possible.

c. CGS-IPS will not directly manage personal devices purchased by employees; however, GN employees are expected to adhere to the same security and information protocols used by the GN when using remote access technologies for connection to the GN network from personal devices. Failure to do so can result in immediate suspension of all network access privileges so as to protect the government's infrastructure.

3. Acceptable Use

a. It is imperative that employees using mobile devices owned by the GN to conduct business, do so appropriately, responsibly and ethically. Based on this requirement, the following rules must be observed:

I. In the event that an employee makes or receives personal calls, or uses data on a GN device that results in excessive costs, the employee may be asked in writing to reimburse the government for all excess costs incurred within 30 days of notification.

II. In accordance with other existing employee policies, no employee is to use a GN owned mobile device for the purpose of illegal transactions, harassment, obscene or inappropriate behavior.

III. If a government-owned mobile device is damaged, lost, or stolen, it must be reported immediately (refer to the Security section below).

IV. If a government-owned mobile device is damaged, lost, or stolen through the gross negligence of the authorized user, that individual may be responsible for reimbursing the government for all repair or replacement costs.

V. If an authorized user does not return a government-owned device when requested or after employment is terminated, he or she may be required to reimburse the government the replacement price of the device.

VI. Users of GN mobile devices must ensure appropriate usage of devices that meet and maintain professional etiquette.

Failure to do so can result in immediate suspension of that user's account.

4. Security

a. GN users assigned a device are accountable for security and privacy due diligence regarding all GN data, communications and government information transmitted through the use of their assigned device.

b. All GN wireless communications records shall be subject to all laws, policies and procedures that apply to the management of any other GN information or record. As per the *Archives Act* every decision and communication with respect to GN-related business must be documented and accessible based on records management retention schedules and/or under the provisions of the *Access to Information and Protection of Privacy Act*.

c. All users must adhere to the following security measures:

   i. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. Where technically possible, **all mobile devices must be protected by an appropriate password**. Employees agree never to disclose their passwords to anyone.

   ii. All users of mobile devices **must employ reasonable physical security measures**. Users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use.

   iii. In the event of a lost or stolen GN managed mobile device, it is the user's responsibility to report the incident to CGS-IPS and their account managers immediately. If the device has been setup to connect to GN resources, where possible, the device will be remotely wiped of all data and locked to prevent access by anyone other than CGS-IPS. The remote wipe will destroy all data on the device, whether it is related to government business or personal.

   iv. Any non-corporate devices used to synchronize or back up data on mobile devices must have installed **up-to-date anti-virus and anti-malware software.**

v. Where CGS-IPS manage mobile devices, this will include the management of security policies, network, application, and data access centrally using the technology solutions it deems suitable. **Any attempt to contravene or bypass that security implementation will be considered non-compliance with the *Acceptable Use of Mobile Devices Policy***.

5. Non-Compliance

a. Failure to comply with the *Acceptable Use of Mobile Devices Policy* may result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment, at the full discretion of the government.

b. The Corporate Chief Information Officer of the Department of Community and Government Services will be advised of breaches of this directive and will be responsible for appropriate remedial action. Any employee discipline shall be in accordance with the policies set forth in the GN *Human Resources Manual*.

ROLES AND RESPONSIBILITIES

1. Executive Council

   a. This policy is issued under the authority of the Executive Council.

2. Minister of Community and Government Services

   a. The Minister of CGS is accountable to the Executive Council for the implementation and administration of this policy.

3. Deputy Minister of Community and Government Services

   a. The Deputy Minister of CGS is responsible to the Minister of CGS for the administration of this policy.

4. Deputy Ministers (all departments)

   a. Deputy Ministers of each department are responsible to ensure that their staff are aware of and required to adhere to this policy.

   b. Deputy Ministers of each department may make decisions regarding the provision of mobile devices to departmental in accordance with this policy and any related operational guidelines.

PREROGATIVE OF CABINET

Nothing in this policy shall in any way be construed to limit the prerogative of Cabinet to make decisions or take action respecting the acceptable use of mobile devices of the Government of Nunavut outside the provisions of this directive.

SUNSET CLAUSE

This policy shall be in effect from the date of the signature until August 31, 2021.

_____

Premier