ACCEPTABLE USE OF MOBILE DEVICES POLICY

POLICY STATEMENT

This Acceptable Use of Mobile Devices Policy (Policy) establishes specific requirements relating to the use of mobile devices to access government information and the protection of such information.

1. PRINCIPLES

This Policy was developed in the spirit of the following Inuit Qaujimajatuqangit Principles:

- **Pijitsirniq**, serving and providing for family and/or community: Managing information in a manner that supports the delivery of government programs and services and protects the rights of Nunavummiut.
- **Pilimmaksarniq/Pijariuqsarniq**, development of skills through observation, mentoring, practice, and effort: Supporting personnel to carry out their responsibilities by providing guidance and direction necessary to protect information.
- **Piliriqatigiinniq/Ikajuqtigiinniq**, working together for a common cause: Ensuring that personnel have the tools required to effectively perform their duties.

2. APPLICATION

2.1. This Policy applies to all users, defined as:

i) government bodies (GB or GBs) and their personnel, and

ii) external entities, including their representatives, contracted to provide services to a GB.

who use a mobile device to access government information or information technology (IT) resources.

2.2. It is the user's responsibility to read and understand this Policy and to conduct their use of mobile devices in accordance with its terms.

3. DEFINITIONS

Company Portal - The application the Government of Nunavut (GN) subscribes to which permits authorized users to access and download GN applications and resources onto a mobile device (e.g., Intune Company Portal).

Deputy Head - Means (a) in relation to a department, the Deputy Minister of that department, and (b) in relation to other government bodies, the person designated as the deputy head.

Government Body (GB) - Means (a) a department, branch or office of the Government of Nunavut, (b) an agency, board, commission, corporation, office or other body designated in the regulations, or (c) the office of a member of the Executive Council as defined by the *Archives Act*.

IT Resources - Means IT resources provided and managed by CGS Information Management/Information Technology Branch (IM/IT) which include, but is not limited to, the infrastructure, network, internet, systems, applications, software, hardware, social media, cloud services, communications tools and devices regardless of the form or format in which such resources were developed, licensed, procured or accessed.

Mobile Device - Mobile devices are computing devices in a small form factor that have at least one network connection interface, non-removable and/or removable storage, and are portable (i.e., non-stationary). These devices come in various forms such as: smartphones, other mobile phones, personal digital assistants (PDAs), tablets, laptops, and wearable devices. Mobile devices include government issued mobile devices and personal mobile devices.

Mobile Device Management (MDM) - Mobile Device Management is the process of managing mobile devices, largely in terms of usage and security usually through the use of a tool or software.

Network - Means any connectivity solution provided by the GN and managed by CGS IM/IT. A corporate network means a wired or wireless connection which has direct access into GN applications and services. A non-corporate network means a wired or wireless connection which does not have direct access to GN applications.

Personnel - Means any individual employed, contracted, seconded, or otherwise providing services to a government body on a full-time, part-time, casual, or volunteer basis.

User - Means as defined in Section 2.1 of this Policy.

4. ROLES AND RESPONSIBILITIES

4.1. Executive Council

This Policy is issued under the authority of the Executive Council. The authority to approve revisions to the Policy rests with Executive Council.

4.2. Minister, Community and Government Services (CGS)

The Minister of CGS is accountable to the Executive Council for the implementation of this Policy.

4.3. Deputy Minister, CGS

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

4.4. Deputy Heads

a) Each Deputy Head (or designate) is responsible for ensuring that all personnel within their government body are aware of and comply with this Policy.

b) Deputy Heads may make decisions regarding the provision of mobile devices to personnel in accordance with this Policy and any related operational guidelines.

4.5. Corporate Chief Information Officer of CGS (CCIO)

a) The CCIO is responsible to the Deputy Minister of CGS for the oversight, operational implementation, and review of this Policy.

b) The CCIO may authorize exemptions to this Policy, or delegate such authorization as required.

4.6. CGS Director of Information Communications Technology (ICT)

a) The CGS Director of ICT shall recommend revisions to this Policy as necessary to reflect technology and information management changes, and ensuring that the Policy aligns with national standards, industry best practices, and all applicable GN policies and legislative requirements.

b) The CGS Director of ICT shall monitor compliance with this Policy.

4.7. Users

Users are responsible for reviewing and understanding this Policy and conducting their role responsibilities and all actions in accordance with its terms.

5. PROVISIONS

5.1. General

a) GBs may routinely assign or provide personnel with access to mobile devices where it is necessary for the effective performance of their official duties.

b) GBs must follow GN processes and procedures governing the procurement of mobile devices for GB personnel.

c) Mobile devices shall only be used in a manner which protects IT resources and the information stored therein and in compliance with all applicable policies and legislative requirements.

d) Only CGS IM/IT approved mobile devices and operating systems may be connected to a GN corporate network or utilize IT resources, which may include only specific versions of such operating systems.

e) All mobile devices accessing a GN corporate network must be centrally managed by CGS IM/IT through a mobile device management (MDM) solution. Mobile devices may access IT resources (e.g., GN email) through portal.office.com without connecting to a GN corporate network or by using the MDM solution when applicable.

f) Laptops connected to a GN corporate network must be configured by CGS IM/IT to ensure the security of such devices.

g) CGS IM/IT reserves the right to refuse, by physical or non-physical means, the ability to connect mobile devices to a GN network (corporate or non-corporate)

or IT resources. The GN will engage in such action if the device(s) being used in any way puts the government IT resources or information at risk.

h) CGS IM/IT uses audit trails, which will be accessed and used without notice by CGS IM/IT for the purpose of protecting the GN infrastructure. Such trails will be able to track the attachment of an external device to the GN infrastructure, and the resulting reports may be used for investigation of possible breaches and/or misuse. A user's connection to the GN infrastructure may be monitored to record dates, times, duration of access, etc., to identify unusual usage patterns or other suspicious activity.

5.2. Acceptable Use

a) When utilizing mobile devices, users will ensure appropriate usage of the device that meets and maintains professional etiquette at all times.

b) Users are responsible for the privacy and security of all the communications and government information transmitted through the use of their mobile devices.

c) Users will only store government information on mobile devices in applications downloaded from the Company Portal.

d) Users will properly manage, and store electronic communications and decisions made on mobile devices in accordance with government records and information management policies and requirements.

e) Where technically possible, mobile devices must be protected by an appropriate password. Users will not disclose their mobile device passwords to anyone.

f) Users will uninstall the MDM solution from mobile devices prior to travelling outside of Canada or the United States with such devices, or such other locations as identified by CGS IM/IT. Non-compliance with this requirement will result in an automatic user account suspension until a cybersecurity investigation is completed.

5.3. Unacceptable Use

a) No mobile device shall be directly connected to the GN corporate network or utilize IT resources without prior approval from CGS IM/IT.

b) Users shall not install applications on government issued mobile devices which have not been authorized by CGS IM/IT.

c) Users shall not store unencrypted passwords on mobile devices.

d) Users will not alter the CGS IM/IT security measures installed or configured on mobile devices.

e) Users shall not plug Universal Serial Bus (USB) drives (e.g., a flash drive, stick, key) into government issued mobile devices, such as laptops, that have executables, software, or movies or any other content which may have come from an untrusted source.

f) Users shall not use a government issued mobile device or personal mobile device connected to the GN network (corporate or non-corporate) or IT

resources for the purpose of illegal transactions, harassment, obscene or inappropriate behavior.

5.4. Use of Personal Devices

a) Personal devices (also referred to as Bring Your Own Device or BYOD) will only be permitted to access IT resources when such devices have installed and utilize the security tools required by CGS IM/IT.

b) Personal devices will utilize the Company Portal or similar technology approved by CGS IM/IT to segregate government information stored on personal devices.

c) CGS IM/IT will manage the segregated portion of the personal device as required to ensure the security of government information.

d) Users 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 non-corporate network from personal devices.

e) Failure to implement proper security measures can result in immediate suspension of all network access privileges so as to protect the government's infrastructure and information.

f) Government information contained in the segregated portion of the mobile device will be automatically backed up and synchronized by the MDM solution. Users are not permitted to backup or synchronize the segregated portion of the mobile device with any other device.

g) The CGS IM/IT Help Desk will not provide support for personal devices except as directly related to the Company Portal and security tools required by CGS IM/IT.

h) Users wanting to utilize their personal devices will be required to review and agree to the terms relating to such use. CGS IM/IT will inform users regarding what aspects of the personal device CGS IM/IT will be able access and manage. Depending on the tool utilized by the GN, CGS IM/IT may be able to see certain device information such as device owner, name, serial number, model, manufacturer, operating system and version, IMEI and app inventory.

5.5. User Responsibility for Mobile Devices

a) Users are expected to secure all mobile devices against being lost, stolen or destroyed, whether or not they are actually in use. Mobile devices must not be left unattended in vehicles or checked into carrier luggage systems.

b) In the event of a lost, stolen, or destroyed mobile device, users will immediately report the incident to their manager and the CGS IM/IT Help Desk. If the device contains or may contain personal information, then the incident must also be reported to the GB's *Access to Information and Protection of Privacy Act* representative in accordance with any policies related to privacy breach notification. In accordance with the security requirements set out in this Policy, lost, stolen, or destroyed government issued devices will be remotely wiped; lost, stolen, or destroyed personal devices which utilize MDM solution will have the segregated portion of the device remotely wiped.

c) Users may be responsible for any personal calls or data usage that result in excessive costs.

d) Any mobile device provided by a GB belongs to the government and must be immediately returned with peripherals (e.g., adapters or chargers) upon request or upon termination of the user's role with the government. If an authorized user does not return the items when requested or after employment is terminated, they may be required to reimburse the government for the replacement value of such items.

5.6. Security

a) CGS IM/IT will determine the security requirements suitable for the protection of mobile devices and the information contained therein. Any attempt by a user to contravene or bypass such security requirements will be a breach of this Policy.

b) The minimum security requirements applicable to each mobile device will be determined by the type of device, permissible security features, and whether such device connects to a GN network (corporate or non-corporate). Minimum requirements include, but are not limited to the following:

i. All mobile devices that access or contain any government information must be password protected or locked by another security method (e.g., biometrics).

ii. All government issued laptops connected to the GN corporate network must be encrypted in accordance with CGS IM/IT's encryption requirements and use multi-factor authentication.

iii. All mobile devices should be set to automatically lock after being idle for a period not to exceed two (2) minutes.

c) CGS IM/IT will manage mobile devices which connect to a GN network (corporate or non-corporate) or utilize IT resources through the use of the MDM solution as applicable.

d) The MDM solution will allow CGS IM/IT to:

i. Control access to GN corporate network and IT resources.

ii. Control use of synchronization services, such as backups, for mobile devices.

iii. Wipe government issued mobile devices when necessary to protect government information. The remote wipe will destroy all data on the device, whether it is related to government business or personal.

iv. Wipe government information from personal devices that utilize the Company Portal to segregate the government information from the user's information (e.g., pictures, personal email application). The remote wipe will only destroy information in the government segregated portion of the mobile device.

e) Mobile devices may not access a GN network (corporate or non-corporate) unless their operating environment integrity is verified (including whether the device has been rooted/jailbroken).

f) The GN shall manage all mobile devices by:

i. Implementing specific device policies and configurations as required to protect the GN networks and infrastructure.

ii. Developing and implementing processes which check for upgrades and patches to the software components, and for appropriately acquiring, testing, and deploying the updates to government issued devices.

iii. Reconfiguring access control features as needed based on factors such as policy changes, technology changes, audit findings, and new security needs.

iv. Detecting, documenting, and reporting anomalies which may indicate malicious activity or deviations from policy and procedures.

v. Incorporating reference to mobile device security practices into CGS IM/IT's security and awareness training.

5.7. Compliance

a) Violation of this Policy may result in suspension of access privileges, disciplinary, and/or legal action leading up to, and including, termination of employment in accordance with GN policies and the Human Resources Manual or termination of service agreement in accordance with its terms. Personnel may also be held personally liable for loss or damage, of equipment assigned to their care, caused by any violation of this Policy in accordance with any applicable Financial Administration Manual Directives.

b) If compliance with this Policy is not feasible or technically possible, or if deviation from this Policy is necessary to support a business function, an exemption request must be submitted by the user's Director to the CGS IM/IT Help Desk. If an exemption is approved, it will be formally documented in accordance with CGS IM/IT's procedures including any limitation to the exemption (e.g., the period of exemption).

6. PREROGATIVE OF EXECUTIVE COUNCIL

Nothing in this Policy shall in any way be construed to limit the prerogative of Executive Council to make decisions or take action respecting the management and use of mobile devices provided by the GB or connecting to GN IT resources outside the provisions of this Policy.

7. SUNSET CLAUSE

This Policy shall be in effect from the date of the signature until August 31, 2027.