ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES POLICY

POLICY STATEMENT

This Acceptable Use of Information Technology Resources Policy ("Policy") establishes specific requirements governing the use of Government of Nunavut ("GN") information technology ("IT") resources. Appropriate organizational use of information technology ("IT") resources and effective security of those resources require the participation and support of the government's workforce. Inappropriate use exposes the government to potential risks including virus attacks, compromise of network systems and services, and legal issues.

1. PRINCIPLES

This Policy was developed in the spirit of the following Inuit Qaujimajatuqangit -Inuit traditional value concepts:

- **Pijitsirniq**, serving and providing for family and/or community: Managing IT resources 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 utilize IT resources.
- **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 have access to the government IT resources as defined below.

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

2.3. This Policy is intended to meet the requirements of the Collective Agreement(s) between the Government of Nunavut and the Nunavut Employee Union.

3. DEFINITIONS

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 Community and Government Services Information Management/Information Technology (CGS 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 (BYOD) mobile devices.

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

i) government bodies (“GB” or “GBs”) and their personnel; and
ii) external entities, including their representatives, contracted to provide services to a GB,

who have access to the government IT resources.

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

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

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) CGS Director of ICT shall recommend revisions to this Policy as necessary to reflect technology and information management changes, and ensuring that it 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 the 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) Use of IT resources and the information contained therein may be monitored, intercepted, read, copied, accessed or captured in any manner including in real time, and used or disclosed in any manner permitted by law, by authorized GN personnel, without additional prior notice to users.

b) Access requests under the *Access to Information and Protection of Privacy Act*, compliance with legal obligations, or issues identified during the government's maintenance and system administration routines may require the disclosure of the information contained in IT resources to appropriate authorities.

c) The GN may impose restrictions, at the discretion of CGS IM/IT management, on the use of a particular IT resource. For example, the GN may block access to certain websites or services that do not serve legitimate business purposes; that negatively impact network performance; or could affect the security of the GN infrastructure.

d) All IT related purchases must be reviewed and approved by CGS IM/IT management through the standard procurement process.

e) Users accessing IT resources through mobile devices must only do so in accordance with the Acceptable Use of Mobile Devices Policy.

f) All users must undergo the security awareness training provided by CGS IM/IT.

5.2. Acceptable Use

a) All uses of IT resources must comply with government policies, standards, procedures, and guidelines, as well as any applicable contractual agreements (e.g., license agreements) and applicable laws.

b) Consistent with the foregoing, the acceptable use of IT resources encompasses the following duties:

- Use of IT resources to perform job-related activities, including communicating with others within the context of the user's assigned responsibility;
- Protecting IT resources and the information contained therein from unauthorized use or disclosure;
- Observing authorized levels of access and utilizing only approved IT devices and services;
- Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information; and
- Immediately reporting suspected information security incidents or weaknesses to the appropriate manager and the CGS IM/IT Help Desk.

5.3. Unacceptable Use

a) The following list is not intended to be exhaustive but is an attempt to provide a framework for activities that constitute unacceptable use.

b) Unacceptable use includes, but is not limited to, the following:

- Unauthorized use of government IT resources;
- Providing access to confidential information, belonging to or held by the government, or personal information, in the custody of the government, without appropriate authorization and in accordance with applicable legislation;
- Distributing, transmitting, posting, uploading, or storing any electronic communications, material or correspondence that is threatening, abusive, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, intentionally false or inaccurate, or otherwise objectionable;
- Posting, transmitting, uploading, or otherwise distributing chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted content using IT resources;
- Deliberately using IT resources to access inappropriate internet sites including those that contain sexually explicit or pornographic material or gambling activities;

- Attempting to use IT resources to represent the government in matters unrelated to official authorized job duties or responsibilities;
- Connecting unapproved devices to the government's network or any IT resource;
- Connecting government IT resources to unauthorized networks;
- Connecting to a non-sanctioned wireless network while physically connected to the government's wired network;
- Plugging in USB drives (e.g., a flash drive, stick, key) into government issued devices that have executables, software, or movies or any other content which may have come from an untrusted source;
- Installing, uploading, downloading, or running any application or software that has not been approved following appropriate security and legal review in accordance with government policies;
- Connecting to or using personal email accounts (e.g., Gmail, Hotmail, Yahoo), storage, or tools not approved by the GN to store or transmit government information or conduct any government business;
- Using IT resources to circulate unauthorized solicitations or advertisements for non-governmental purposes including, but not limited to, religious, political, or not-for-profit entities;
- Providing unauthorized third parties, including family and friends, access to the government's IT resources, information, or facilities;
- Using IT resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions, crypto mining);
- Connecting to commercial file sharing sites (e.g., Dropbox) that have not been authorized for the upload or storage of government information;
- Tampering, disengaging, or otherwise circumventing the government's or a third-party's IT security controls;
- Attempting to access any IT resource, account, or information without the authorized right to do so;
- Engaging in any activity that intentionally restricts, disrupts or degrades the government's ability to deliver a service, including, but not limited to, the transfer of large amounts of material or any other use that inhibits the performance of a service or jeopardizes data security;
- Engaging in any activity which, regardless of the purpose, constitutes appropriation of another person's identity;
- Knowingly post, transmit or otherwise distribute a virus, bug, malicious code, "Trojan horse", "worm" or other harmful or disruptive data;
- Knowingly attempt to bypass government security measures and procedures; and

- Knowingly incurring charges or expenses through inappropriate use of communication tools or devices (e.g., unauthorized long distance calls).

5.4. Occasional and Incidental Personal Use

a) Occasional, nominal, and incidental personal use of email and the internet is permitted in accordance with Article 14 of the Nunavut Employees Union Collective Agreement, provided such use: is otherwise consistent with this Policy; is limited in amount and duration; does not interfere with the performance of the user's duties and responsibilities; and does not impede the ability of other users to fulfill their respective duties and responsibilities. Exercising good judgment regarding occasional, nominal, and incidental personal use is important.

5.5. Individual Accountability

a) Individual accountability is required when accessing all IT resources. Everyone is responsible for protecting against unauthorized activities performed under their user credentials (e.g., ID, passwords, tokens or similar technology). This includes locking your computer screen when you walk away from your system, and protecting your credentials from unauthorized disclosure. Credentials must be treated as confidential information, and must not be disclosed or shared.

b) Passwords utilized to access IT resources must not be the same as passwords used to access personal devices and applications, including social media sites, in order to prevent unauthorized access to IT resources if the password is compromised.

5.6. User Responsibility for IT Equipment

a) Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to the government and must be immediately returned upon request or upon termination of the user's role with the government.

b) Devices containing government information must be attended to at all times or physically secured; devices must not be left unattended in vehicles, or checked into carrier luggage systems.

c) Should IT equipment be lost, stolen or destroyed, users are required to 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 *ATIPP* representative.

5.7. Access

a) User credentials and access to IT resources is provided based on the user's role and responsibilities within a GB or contracted organization.

b) When a user changes roles or transfers to another GB, such user must cease to access and use credentials provided for the previous role.

c) A user shall not access IT resources upon termination of employment or the contract under which the user was providing services, as applicable.

d) It is the responsibility of the user's supervisor to notify the CGS IM/IT Help Desk about any changes to a user's role, including any extended leave of absence, termination of employment, or expiration of the contract under which the user was providing services. The CGS IM/IT Help Desk must be notified prior to the effective day of the change to the user's role. (i.e., CGS IM/IT must be able to affect change prior to date of termination).

e) Closed user accounts will be archived in accordance with GN policies and procedures and no longer accessible, except where the account is to be accessible during a pre-authorized transition period.

5.8. Multi-Factor Authentication

a) Users will utilize a multi-factor authentication method (e.g., YubiKey) approved by the government to access IT resources.

b) Users shall not share or permit any other individual to use their multi-factor authentication method.

c) Users that transfer to a new department or GB, shall have their multi-factor authentication reset and registered to their new account.

5.9. Virtual Private Networks (VPNs)

a) Users will not be permitted to access IT resources unless CGS IM/IT can validate that the user is coming from a legitimate internet protocol (IP) address or device.

b) Personal VPNs will be flagged by CGS IM/IT security tools and autoblocked.

c) VPNs, anonymizers, proxies and third-party tools that are used to access or bypass GB security tools and restrictions are strictly prohibited.

5.10. Third Parties/External Parties

a) No external party shall be provided with access to government IT resources unless such party has signed an agreement, with a defined start and end date, which includes appropriate terms governing the services provided and use of IT resources in accordance with this Policy.

5.11. 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 use of IT resources of the Government of Nunavut, outside the provisions of this Policy.

7. SUNSET CLAUSE

This Policy will be effective from the date of signature and shall be reviewed every four (4) years or sooner to address significant technology or business process changes.

The government has an obligation to consult the Nunavut Employees Union regarding any changes to this Policy or its guidelines, as per Article 14 of the Nunavut Employees Union Collective Agreement.