City of St. John's Corporate and Operational Policy Manual

Policy Title: Information Technology Policy	**Policy #:** 02-01-18
Last Revision Date: N/A	**Policy Section:** Information Technology>Information Technology
Policy Sponsor: Deputy City Management, Finance and Administration	

1. Policy Statement

The City is committed to the efficient and safe use of its IT resources and to maintaining the security of its IT systems.

2. Definitions

"Authorized User" means an Employee who supports the operations and integrity of City IT resources and their use, and who has administrative-level access to IT resources not accessible by regular Users.

"Department Head" means all Deputy City Managers (DCMs) and the City Manager or their designate.

"Direct Supervisor" means a City management Employee to whom another Employee directly reports.

"Employee" means any person employed by the City of St. John's as a permanent, term, part-time, casual, contract, seasonal, temporary, or student worker.

"Information Technology" ("IT") includes, but is not limited to computers, systems, mobile communication devices, electronic communication, VOIP telephony, servers, applications, data, software tools, electronic access accounts, information assets, technology acquisition, technology standards and processes, network resources, and overall business technologies and infrastructure.

"User" means an Employee, Member of Council, or other authorized person using City IT resources.

"Security Incident" means any event in which electronic data has been improperly accessed, disclosed, altered, or destroyed.

3. Policy Requirements

3.1 Acceptable Technology Use

a) IT resources shall be reserved for conducting City business, with the exception of occasional personal use provided that such personal use is not excessive, does not negatively impact work productivity, and/or does not negatively interfere with work performance, as further detailed in the **Information Technology Procedures**.
b) Users shall use City IT in accordance with all applicable legislation, policies, and/or procedures, including:
   i. Access to Information and Protection of Privacy Act, 2015,
   ii. Asset Management Policy,
   iii. Code of Ethics By-Law,
   iv. Privacy Management Policy,
   v. Records and Information Management Policy,
   vi. Respectful Workplace Policy,
   vii. Corporate Social Media Usage Policy, and
   viii. Fraud Policy.

3.2 Physical IT Resources and Electronic Data

3.2.1 Physical IT Resources and IT Support

a) Users shall be provided with appropriate IT resources by the Corporate Information Services Division.
b) Acquisition of IT resources shall be pre-approved by the Corporate Information Services Director or designate, in cooperation with the Supply Chain Division.
c) All IT provided to Users and/or created/modified by Users as part of their employment shall remain the property of the City.
d) IT resources shall be managed and IT support shall be provided as detailed in the **Information Technology Procedures.**

e) The City shall not support any “Bring Your Own Device” programs.

3.2.2 Electronic Data

a) Users shall minimize the security risks that their IT use poses to the City, as detailed in the **Information Technology Procedures**.
b) Local or remote access to the City network by Users shall be authorized by an Employee’s Direct Supervisor; reviewed and approved by the Corporate Information Services Division; and shall be conducted on a Corporate Information Services Division-approved IT device.
c) All electronic records shall be managed and maintained in accordance with all applicable legislation, policies, and/or related procedures.
d) All IT solutions and procurement of IT solutions, including cloud solutions, shall comply with all applicable legislation, policies, and/or procedures, including those noted in the **Information Technology Procedures**.

3.3 Information Security and System Administration

a) IT security and system administration shall comply with the **Information Technology Procedures**.
b) Standards for approved security software and configurations shall be set by the Corporate Information Services Division.
c) Where audit functionality exists within an IT system, it shall be used.
d) Authorized Users shall only use their privileges in the performance of their duties and shall not use these privileges to access IT resources or data that would otherwise be inaccessible and shall not access data and/or information without necessary approvals from the Corporate Information Services Director or designate.

3.3.1 User Information and Network Security

a) Users shall only use IT hardware authorized by the CIS Division if connection to City IT systems is required. For other IT requirements, Users shall consult with the Corporate Information Services Division.
b) Users shall comply with all applicable copyright and license requirements and shall comply with the prohibitions detailed in the **Information Technology Procedures**.

3.3.2 User Account and Access Management

a) Authorized access to IT systems shall be at the minimum level required for the User to perform and complete their assigned duties, subject to software limitations for account management.
b) Direct Supervisors or designates shall complete requests for access or requests to change/remove access (including when a User's employment, contract or term ends or a User changes positions) as detailed in the **Information Technology Procedures**.
c) Electronic data management in the event of unexpected or extended absence by a User; management of shared or generic IT accounts; and User system access review shall comply with the processes detailed in the **Information Technology Procedures**.

3.3.3 Security Incidents

a) In the event of a Security Incident or suspected Security Incident, Users shall follow the requirements as detailed in the **Information Technology Procedures**.

3.4 Privacy Rights

a) The City recognizes that Users have a reasonable expectation of privacy related to their IT use and that this expectation shall be balanced against the organization's management rights.
b) The City reserves the right to monitor, duplicate, record, and/or log all User content or use of City IT resources with or without notice, within the parameters detailed in the **Information Technology Procedures**, in order to support operational requirements (including maintenance and security), internal investigations, audits and/or fraud investigations, or law enforcement requests. Any such examination shall be consistent with a User's privacy rights and the least intrusive means shall be used where possible and appropriate.

3.5 IT Printing

a) The use of shared printing and multifunctional devices in the workplace and requirements for printing work-related documents from an Employee's personal home printer shall comply with the **Information Technology Procedures**.

3.6 Acknowledgement

a) All Users shall read and comply with the conditions of the policy terms.
b) Other authorized Users who require IT resource access or who deliver cloud-based solutions (including, but not limited to contractors/ suppliers) shall agree to comply with the policy as part of their contract or agreement.

3.7 Exceptions

a) The Corporate Information Services Division shall have the authority to provide, and Users may request, exceptions to specific provisions of this policy based upon unique business requirements and other considerations, as detailed in the **Information Technology Procedures**.

4. Application

This policy applies to all Users and all IT owned or leased by the City and IT that is not owned by the City but is certified, contracted, or permitted to connect and access the City IT systems through approved processes or remote access tools, but shall not apply to the St. John's Transportation Commission (Metrobus).

5. Responsibilities

5.1 The Corporate and Information Services Division shall be responsible for:

a) the overall implementation and compliance monitoring of the policy and any associated procedures;
b) supporting departments with their IT resource requirements, as required;
c) managing connectivity and security for IT administered by the Corporate Information Services Division;
d) approving or denying requests for exceptions to the policy.

5.2 Department Heads shall be responsible for:

a) complying with the policy and procedures and making their Employees, including those Employees who are Direct Supervisors, aware of the policy and procedures;
b) directing Employees who administer the department's own IT consult with the Corporate Information Services Division to allow IT system and security requirements and IT best practices to be considered;
c) directing that the Corporate Information Services Division be consulted prior to departmental procurement of IT.

5.3 Direct Supervisors shall be responsible for:

a) being aware of, complying with, and advising their Users of the requirements of the policy and its procedures;
b) submitting IT access change requests to the Corporate Information Services Division in a timely manner; and
c) returning all City-issued IT to Corporate Information Services Division following the end of an Employee's employment.

5.4 Users shall be responsible for:

a) complying with this policy and any associated procedures.

6. References

- Access to Information and Protection of Privacy Act, 2015
- Asset Management Policy
- Corporate Social Media Usage Policy
- Fraud Policy
- Information Technology Procedures
- Privacy Management Policy
- Procurement Policy
- Records and Information Management Policy
- Respectful Workplace Policy
- St. John's Code of Ethics By-Law

7. Approval

- Policy Sponsor: Deputy City Manager, Finance and Administration
- Policy Writer: Director, Corporate Information Services; Supervisor, Application Management; Supervisor, Infrastructure; Policy Analyst
- Date of Approval from
    - Corporate Policy Committee: April 19, 2021
    - Senior Executive Committee: February 18, 2022
    - Committee of the Whole: February 23, 2022
- Date of Approval from Council: March 7, 2022

8. Monitoring and Contravention

a) The Corporate Information Services Division shall monitor the application of the policy.
b) Any contravention of this policy and/or associated procedures shall be reported to the Department of Finance and Administration (including the Human Resources Division), the Office of the City Solicitor, and/or the City Manager for further investigation and appropriate action.
c) Appropriate action may include, but is not limited to, access termination, legal action, and/or discipline up to and including dismissal and for authorized external users, appropriate action may include, but is not limited to, suspensions or termination of their contract/agreement.

9. Review Date

Initial Review: 3 years, Subsequent Reviews: 5 years.