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

Procedure Title: Information Technology Procedures	
Authorizing Policy: Information Technology Policy	
Last Revision Date: N/A	**Procedure #:** 02-01-18-01
Procedure Sponsor: Director, Corporate Information Services	

1. Procedure 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. Procedure Requirements

3.1 Acceptable Use

As noted in Section 3.1(a) of the policy:

a) Users are encouraged to ask their Direct Supervisor or submit a request to the IT Helpdesk if they have any question regarding the appropriate use of IT. A non-exhaustive list of acceptable and unacceptable use is contained in Annex A.

3.2 Physical IT Resources and IT Support

As noted in Section 3.2.1(d) of the policy:

a) Direct Supervisors shall obtain all City-issued IT for Employees reporting to them who cease employment with the City. The Office of the City Clerk shall obtain City-issued IT from that Members of Council at the end of their respective term. Any returned City-issued IT shall be forwarded to the Corporate Information Services Division.
b) The Corporate Information Services Division shall only provide support for City-issued IT. IT support shall only be available from 8:00am to 4:30pm, Monday to Friday, unless urgent intervention is required.
c) Users shall be responsible for the security of IT physically under their control and shall exercise reasonable care to prevent damage or theft.
d) Users shall secure City issued laptops with City issued cable locks at all times.
e) Users shall report theft or damage to any IT physically under their control immediately to their Direct Supervisor and to the IT Helpdesk via phone or email.
f) The Corporate Information Services Division shall maintain an inventory of all physical IT, in cooperation with the Program Manager, Asset Management.

Commented [KSB1]: Rec 3.12(ii)

g) Under no circumstances shall Users insert unknown or found removeable media into City issued devices. If Users require a removable device, such as a USB device, for business purposes, they shall contact the Information Services Help Desk.

Commented [KSB2]: Rec 4.1

3.3 Electronic Data Protection

As noted in Section 3.2.2(a) of the policy, Users shall minimize security risks that their IT use poses to the City and shall:

a) not store City-owned information on unauthorized IT devices;
b) check with the Corporate Information Services Division before using any removable IT media (e.g., USB drives) that are not City-approved or issued;
c) encrypt any personal or confidential information stored on removable IT media;
d) completely delete at the earliest opportunity all information from removable IT media after it is transferred and stored on a City network drive to allow back-up and recovery procedures of City IT resources to be performed;
e) when working on City documents from a non-corporate location, use a City-issued phone as a WiFi hotspot and if the User does not have a City-issued phone, avoid the use of unprotected WiFi; and
f) not conduct City business using their personal electronic accounts (e.g., personal email, personal cloud storage) or send or share digital documents or records to their personal electronic accounts.

3.3.1 Procurement of IT Solutions

As noted in Section 3.2.2(d) of the policy:

a) Prior to procurement of any cloud solutions, a privacy assessment shall be completed by the department in consultation with the Access to Information and Protection of Privacy (ATIPP) Coordinator and is subject to approval by the Corporate Information Services Division and the ATIPP Coordinator. Cloud solutions shall enable City information to be transferred back for storage on the City's technology environment at the end of a contract with the vendor.

3.4 Information Security and System Administration

As noted in Section 3.3(a) of the policy, IT security and system administration shall be as detailed below.

a) For all IT administered by the Corporate Information Services Division, security shall be the responsibility of the Corporate Information Services Division. For IT administered by other departments, security shall be the responsibility of the individual department/division, in consultation with the Corporate Information Services Division.
b) For IT with any financial functionality or capability, the Department shall consult with the Financial Services Division and the Corporate Information Services Division regarding security requirements.
c) Authorized Users shall install security and device management software on all IT resources administered by the Corporate Information Services Division.
d) For all IT administered by the Corporate Information Services Division, Authorized Users shall be responsible for all IT licensing. For IT administered by other departments, individual department/division Employees shall be responsible for the IT licensing, in consultation with the Corporate Information Services Division.

3.5 Prohibited Activities

As noted in Section 3.3.1(b) of the policy, Users shall not:

a) disable or circumvent any controls intended to safeguard IT resources;
b) share any IT account or password information with anyone, including other Users or third parties, with the exception of Authorized Users during the delivery of IT support services, as required, after which it shall be the User’s responsibility to change their password;
c) provide access to the User’s assigned IT to another individual, either deliberately or through failure to secure such access;
d) download or introduce inappropriate content or software with intentions to probe; scan; or cause harm, loss, or damage to the City’s IT;
e) cause a disruption of service to the City’s IT by performing non-business activities including, but not limited to, gaming, audio/video download or play back, storing their own personal data (including, but not limited to, personal photos, music, videos), or moving or disconnecting shared devices under the control of the City; and/or
f) forge, misrepresent, or obscure their User identity on any electronic communication to mislead the recipient.

3.6 IT Systems, Equipment, and Internet Requests

a) As noted in Section 3.3.2(b) of the policy, Direct Supervisors or designates shall complete requests for access or requests to change or remove access to IT systems, equipment, or certain Internet sites using the appropriate method as detailed below.

3.6.1 Data Restoration

a) For any requests for data to be restored, Departments shall submit an email request to the IT Help Desk with the details on the files/folders to be restored.

3.6.2 New or Changed Network Access, Hardware, or Software

a) Departments seeking new or changed network access, hardware, or software (including mobile phones) shall complete the "Network Access, New or Change - Hardware and or Software Request" form. This shall be completed when a User's employment, contract, or term ends; a User changes positions; or as required to address departmental requirements.

   i. The User's Direct Supervisor shall complete the form and if payroll or HR system access is not required, shall submit it via email to the IT Help Desk.

   ii. If Payroll, HR system, or Njoyn access is required, the "Network Access, New or Change - Hardware and or Software Request" form shall be submitted to the Manager, HRIS detailing the role assignment needed. The Manager, HRIS shall review and assign the appropriate role and forward the approved form to the IT Helpdesk for processing.

3.6.3 Deleting or Disabling Network Access

a) Departments seeking to delete or temporarily disable a User's access shall complete the "Network Access - Delete/Disable Request" form. The User's Direct Supervisor shall complete the form and submit it via email to the IT Help Desk.

3.6.4 IT Project Requests

a) Departments seeking to have new IT projects considered for development shall complete the "Project Request Form" and submit it via the electronic “submit form” button in the form or via email to the IT Help Desk.

3.6.5 VPN Access Requests

a) Departments seeking User access to the City's Virtual Private Network (VPN) shall complete the "VPN Access Request" form and send to the IT Help Desk.

3.6.6 Internet Access

a) The Corporate Information Services Division uses filtering tools to restrict Internet access. The User's Direct Supervisor shall submit a request via email to the IT Helpdesk detailing the business need for the access.

3.6.7 VOIP Telephones

a) Requests for new VOIP telephones or changes to existing VOIP telephones shall be submitted the IT Helpdesk using the "Telephone Request Form".

3.6.8 Mobile Phones

a) Requests for new mobile phone service, upgrades, and/or replacements shall be submitted to the IT Helpdesk using the "Cellular Request Form".

3.7 User Account Management

3.7.1 Change or Termination of Employment

As noted in Section 3.3.2(b) of the policy:

a) Direct Supervisors or designates shall request that User access to IT is disabled when a User's employment, contract, or term ends or a User changes positions, by completing the "Network Access - Delete/Disable Request" as noted in Section 3.6.3 of the procedures. Direct Supervisors shall also arrange for User access to any IT directly managed by the Department to be disabled (e.g., cloud solutions).

b) For new or reassigned Employees, Direct Supervisors or designates of the new division shall request User access to required IT for the new or reassigned position by completing the "Network Access, New or Change - Hardware and or Software Request" as noted in Section 3.6.2 of the procedures.

c) Once the Corporate Information Services Division reviews the request, the User account may be modified/disabled.

d) For disabled accounts where a User’s employment, contract, or term ends, if there has been no request by the Department Heads or designates to maintain the accounts within 30 days, the account shall be deleted. The Corporate Information Services Division shall confirm with the Direct Supervisor as to how long the account information should be retained.

3.7.2 Account Access and Management

As noted in Section 3.3.2(c) of the policy:

a) In the event of an unexpected or extended absence by a User, access to the User’s electronic data may be granted to a designated person upon approval by their Department Head or designate, as required to maintain normal business operations.

b) Shared or generic IT accounts shall be limited, where possible. For any shared or generic IT accounts, the manager responsible for the shared account shall be accountable for any inappropriate activities initiated from that shared account.

c) Each Department shall review account access to IT systems (including User access rights within the IT systems) at least annually and shall provide updates to the Corporate Information Services Division. For all IT resources administered by individual departments or divisions, the Department Head or designate shall review that account access to these IT resources (including User access rights within the IT systems) at least annually.

3.8 Security Incidents

As noted in Section 3.3.3(a) of the policy, Employees shall follow the requirements detailed below if an IT resource or system has had unauthorized access, or there is a reasonable suspicion of a Security Incident or other compromise.

a) Authorized Users shall immediately suspend access to the account on the involved IT and any other systems at risk from the Security Incident.

b) Access shall not be reinstated until Authorized Users have reviewed the resource or systems for unauthorized modifications.

c) Any User who becomes aware of a possible Security Incident involving electronic data shall immediately inform their Direct Supervisor and the IT Service Desk at the following contact details:

Email: hdesk@stjohns.ca
Phone: (709) 576-6154
In person: Information Services desk at City Hall 2nd Floor.

Commented [KSB3]: Per rec 8.3(ii)

d) Users shall also report all Security Incidents relating to suspicious or potentially malicious emails by using the Beauceron Report a Phish function in Microsoft Outlook or via email at phish@stjohns.ca.

Commented [KSB4]: Per rec 8.3(i)

e) As soon as the Security Incident has been confirmed to have occurred, the Corporate Information Services Division shall inform the Department Head.

f) If a privacy breach is suspected, the ATIPP Coordinator shall be informed by the Department Head.

3.9 IT Operations, Investigations, and Legal Requests

a) As noted in Section 3.4(b) of the policy, 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 below.

3.9.1 IT Operations, Maintenance, and Security

For the purposes of IT operations, maintenance, or security:

b) The City reserves the right for Authorized Users to revoke or block access and/or usage of any IT, with or without notice, if deemed necessary and if approved by the Corporate Information Services Director or designate.

c) Authorized Users may routinely monitor IT resources for operational, maintenance, or security purposes without requiring additional approvals.

d) For urgent IT maintenance and/or security issues, it may be necessary for Authorized Users to examine user content or use without notice to the User or other departments.

3.9.2 Internal Investigation

a) Prior to seeking approval for the Corporate Information Services Division to respond to any internal request for investigation of User content or use (excluding audit-related requests), Direct Supervisors shall discuss the request with the Human Resources Division to determine whether other action is more appropriate.

b) If retrieval and/or review of User content or use is determined to be warranted in (a), Direct Supervisors shall complete the “Request for IT

Investigation" form and it shall be approved by the Department Head prior to being forwarded to the Department's HR Advisor.

c) If an investigation is to proceed, the HR Advisor shall sign and forward to the Corporate Information Services Director or designate. Authorized Users shall retrieve the User information and shall only examine it to the extent necessary to fulfill the request.

d) It shall be the responsibility of HR Employees to examine the User information as part of their investigation. Authorized Users may provide any necessary support as needed.

3.9.3 Audit and Fraud Investigations

a) Authorized Users may be required to retrieve or review User IT content or use without notice to the User to support the authorized activities of the Office of the City Internal Auditor under the Internal Audit Charter Policy and/or the Fraud Policy.

b) Authorized Users shall retrieve the User information and shall only examine it to the extent necessary to fulfill the request.

c) It shall be the responsibility of Office of City Internal Auditor Employees to examine the User information as part of their investigation. Authorized Users may provide any necessary support as needed.

d) Prior to seeking approval for responding to any external auditing-related requests, the Corporate Information Services Director shall obtain the approval of the DCM, Finance and Administration.

3.9.4 Requests from Law Enforcement

a) Prior to seeking approval for compliance with any requests by law enforcement involving User IT content or use, the Direct Supervisor and/or Authorized Usersshall consult the Office of the City Solicitor to determine any legal requirements.

b) Following consultation with the Office of the City Solicitor, any request for such activity as detailed in (a) shall be approved by the (i) Corporate Information Services Director or designate and the HR Director or designate for all Employees, and (ii) the Corporate Information Services Director or designate for all other Users.

c) Upon approval in (b), Authorized Users shall retrieve the User information and shall only examine it to the extent necessary to fulfill the request.

3.10 IT Printing

As noted in Section 3.5 of the policy:

a) Use of shared printing and multifunctional devices are intended for day-to-day reasonable printing needs. For all large print jobs (that is, more than 100 pages total), Users shall use the City Print Room and may contact the Communications and Office Services Division for additional information.

b) Printer colour usage shall only be applied to final documents. All draft and proofing documents shall be printed in black and white and in draft mode.

c) Requests for replacement/additional printers shall be approved by the Director, Corporate Information Services.

d) Users shall consider their actions to reduce paper printing and print wastage.

3.10.1 Printing from Home

a) Users shall not print any documents from their home printers unless they comply with the requirements detailed below:

    i. Users shall only print files from their online Office 365 account and shall not download any files to their personal IT devices.

    ii. If the file to be printed contains any personal, private, or confidential information, the User shall obtain approval from their Direct Supervisor prior to printing. The User shall protect all personal, private, and/or confidential information at all times.

b) Users are encouraged to minimize their use of home printing for any work documents and consider using digital alternatives.

c) The Corporate Information Services Division shall not be responsible for support for any printing from home.

3.11 Exceptions

As noted in Section 3.6 of the policy,

a) For exceptions, an “Exception to Policy Request” form shall be completed, including valid business justification and approval by the User’s Department Head, prior to forwarding to the Corporate Information Services Division.

b) Exceptions to the policy and procedures shall only be approved by the Corporate Information Services Director or designate.

4. Application

These procedures apply 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 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 IT systems, equipment, and Internet requests.

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;

5.3 Direct Supervisors shall be responsible for:

a) being aware of and complying with, and advising their Users of, the requirements of the policy and its procedures;
b) knowing the access requirements for the applications used by their Users;
c) submitting IT access change requests to the Corporate Information Services Division in a timely manner;
d) advising Users that any Security Incidents needs to be reported to their Direct Supervisor as soon as possible;

e) reporting any Security Incidents reported to them to the IT Helpdesk as soon as possible;

f) periodically monitoring their Users for laptop cable lock compliance in accordance with Section 3.2(d).

Commented [KSB5]: Per rec 3.12(iii)

5.4 Users shall be responsible for:

a) complying with these procedures.

6. References

- Access to Information and Protection of Privacy Act, 2015
- Information Technology Policy
- Internal Audit Charter Policy
- Fraud Policy
- Privacy Management Policy
- Records and Information Management Policy

7. Approval

- Procedure Sponsor: Director, Corporate Information Services
- Procedure 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

8. Monitoring and Contravention

a) The Corporate Information Services Division shall monitor the application of the policy and procedures.

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: 1 year, Subsequent Reviews: concurrent with policy review

Annex A

Acceptable and Unacceptable Use of Technology

A non-exhaustive list of acceptable IT use and unacceptable IT use is provided below.

Examples of Acceptable Use

1. Use of IT to perform activities as a part of the User’s official duties;
2. Use of educational and other applicable websites that further a User’s work knowledge and skills;
3. Streaming of Council meetings or eLearning events;
4. Limited personal use that is conducted on personal time; that is not for financial gain; that does not incur any additional costs for the City; and that does not interfere with City business.

Examples of Unacceptable Use

1. Using City IT for any type of disrespectful behaviour, as detailed in the Respectful Workplace Policy;
2. Using City IT for any type of illegal activity; including but not limited to violating copyright laws and/or contractual obligations (including, but not limited to, illegally duplicating, or transmitting copyrighted or restricted software and content such as data, pictures, music, or video);
3. Buying hardware, software, and/or software services outside of normal City procurement processes;
4. Creating or accessing offensive, indecent, or sexually explicit material;
5. Using City IT for online gaming or gambling;
6. Using City IT for personal commercial purposes, including sending unsolicited commercial electronic messaging, text messages, instant messages, voicemail, or other forms of electronic communication;
7. Interfering with others’ lawful use of data and computers, including but not limited to, destroying, altering, or encrypting data without authorization and with the intent of making the data inaccessible to others who have a lawful need of access;
8. Distributing confidential or knowingly false material;
9. Using City storage for their own personal data (including but not limited to personal photos, music, videos);
10. Emailing City documents or information to personal email accounts.