Information Technology Asset Management Policy

PURPOSE
The purpose of this policy is to ensure that IT Assets at City are managed through an established IT Asset Management Policy and Process. The City will utilize Best Practices and Frameworks (i.e., ITIL) for the implementation of their IT Asset Management Process as it pertains to City IT Systems and Environments.

SCOPE
This Policy applies to City employees, contractors, volunteers, and vendors that access City IT resources (unless otherwise addressed by a current collective bargaining agreement or public safety Policy).

ACRONYMS
City:	City of Vancouver
CI:	Configuration Item
CIS:	Center for Information Security
IRT:	Incident Response Team
ISO:	Information Security Officer
PCI:	Payment Card Industry
TSM:	Technology Services Manager
IT:	Information Technology
ITISPP:	Information Technology Information Security Program Policy
ITISS:	Information Technology Information Security Standards

DEFINITIONS
TBD

BACKGROUND
IT Asset Management is the Process that controls the life cycle of all IT Assets, including Planning, Request, Procurement, Deployment, Management, Transfer, and Retirement.

STATEMENT OF POLICY

General Requirements
1. IT users, to include employees and contract personnel, shall not remove IT assets supplied by City from City premises, except under the following conditions.
   a. IT assets assigned to employees and contractors, which may include laptop computers and Personal Communication Devices, may be removed from City premises as deemed acceptable by City Examples include:
      - ✓ Teleworking / On-Call Activities
      - ✓ Field work that is part of an assigned position
   b. Exceptions to this policy must be documented in writing and approved by the employee's supervisor and by City Approving Authority. Documentation of exceptions shall include:
      - ✓ The business or technical justification;
      - ✓ The scope of the exception, including quantification and duration (not to exceed one year);
      - ✓ A description of all risks associated with the exception;
      - ✓ Identification of controls to mitigate the risks; and
      - ✓ Identification of any unmitigated risks associated with the exception.
2. IT users are responsible for safeguarding any IT assets they remove from City premises, including keeping these assets under their direct physical control whenever possible, and physically securing the assets (i.e., by means of lock and key) when they are not under the IT users direct physical control.
3. IT users must immediately report loss or theft of any assigned IT assets to their supervisor and as appropriate, to City InfoSec within 24 hours of a known occurrence.

4. IT users may bring personal IT assets into City work locations. Personal IT assets may not be connected to City or business partner production network. (PCI Bubble).
    a. In general, connection of personal IT assets is allowed only to networks provided by City for guest or public access.
    b. Exceptions to this policy must be documented in writing and approved by the employee's supervisor and by City Approving Authority. Documentations of exceptions shall include:
        - ✓ The business or technical justification;
        - ✓ The scope of the exception, including quantification and duration (not to exceed one year);
        - ✓ A description of all risks associated with the exception;
        - ✓ Identification of controls to mitigate the risks; and
        - ✓ Identification of all unmitigated risks associated with the exception.
5. All electronic media containing City, Partner, and/or PCI in-scope data whether stored on City assets or that of a service provider, shall have all of that data securely removed from the electronic media as specified by applicable City Information Security Policies before the electronic media is surplused, transferred, traded-in, otherwise disposed of, or replaced.

IT Software Asset Management

1. IT users shall only use City approved and appropriately licensed software on owned, leased, or City provided IT Assets.
2. Installation of software that is not approved or appropriately licensed on owned, leased, or City provided IT assets is prohibited.
3. No less than annually, City Asset Manager or designee shall conduct an audit of software license distribution and reconciliation to verify and validate that all software used by City is appropriately licensed and approved.

Change and Release Management

1. City employees and contractors shall document IT asset configuration and changes to asset configuration at all stages of the system development life cycle.
2. All changes to IT assets used by City or its Partners shall be made in accordance with the City Change and Release Management Policy and at a minimum include the following steps:
    - ✓ Initiate change request
    - ✓ Review and approve change
    - ✓ Build and test change
    - ✓ Create and document back up/back out plan
    - ✓ Implement change
    - ✓ Document change

Compliance

- The Asset Manager will verify compliance to this Policy through various methods, including but not limited to, periodic internal and external scans and feedback to the Policy owner.
- An employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.
- Any exception to the Policy must be approved by the IT Director in writing

RELATED DOCUMENTS

City IT Information Security Program Policy
City IT Information Security Standards
City IT Configuration Management Policy

CONTACT INFORMATION

For questions about this policy, please contact the ISO or the IT Director

VERSION HISTORY

Version History		
Version	Date	Change Summary
1	07/15/2015	Original developed by Braun Tacon as a ITAM policy template
2	04/19/2017	Adapted from template and Adopted by City of Vancouver ISO