PROCEDURES

Title	**Internet of Things**
Policy No.	B.5.5
Approval Body	President & Chief Executive officer
Policy Sponsor	Associate Vice President, Information Technology & Chief Information Officer
Last Revised/Replaces	
Effective Date	February 13, 2020

1. All VCC's Departments or any third party acting on behalf of VCC are required to contact the IT Department prior to acquisition of the new IoT device to avoid network compatibility or security issues.
2. The IT Department will review IoT devices to determine:
    a. Risk to the data or services provided by the device.
    b. Risk to the device itself.
    c. Risk to VCC's computer network or to other VCC's IT systems.
    d. Compliance with FOIPPA and with other relevant legislations.
    e. Network compatibility.
    f. Other Cyber Security risks.
3. Where necessary, the IT Department will consult Facilities; Safety, Security and Risk Management; Purchasing; and other VCC's Departments.
4. The IT Department will determine if the IoT device is safe to connect to VCC's computer network and will approve the IoT device to be purchased and/or to be connected to VCC network.
5. If the IoT device is deemed to be unsafe for VCC, the IT Department will continue to work with the requestor to find a suitable product.
6. No IoT device owned, used, or managed by VCC or on behalf of VCC may be connected to any VCC wired or wireless computer network without proper review and authorization from the IT Department.
7. In case of disagreement with the IT Department's decision, the requestor may escalate to the CIO. The CIO's decision is final.
8. The IT Department will assist with the configuration of the approved IoT devices to ensure safe connectivity to VCC's computer network.
9. The IT Department may monitor VCC's computer network for the presence of unauthorised IoT devices and will disconnect any unauthorised IoT device from the network.

RELATED POLICY

Refer to B.5.5 Internet of Things Policy.