



Title	<b>Internet of Things</b>
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

### **CONTEXT AND PURPOSE**

The purpose of this policy is to set out the guidelines for managing all risks associated with Internet of Things (IoT) devices at Vancouver Community College (VCC; the College).

The purpose of this policy is to outline the approved way of connecting IoT devices to the VCC computer network, and to maintain the confidentiality, integrity and availability of these devices and the entire VCC computer network.

### **SCOPE AND LIMITS**

The Policy applies to any IoT device owned, used, or managed by VCC or on behalf of VCC, which requires connectivity to VCC wired or wireless computer networks. Cellular networks, provided by mobile operators, are not in-scope of the Policy.

### **STATEMENT OF POLICY PRINCIPLES**

1. VCC recognizes the need to use emerging technologies, such as the IoT, to support innovation and exploration in teaching and learning at VCC and to improve VCC's operations.
2. The IT Department is responsible for managing all risks related to IT systems and the computer network, therefore the IT Department will review and approve the purchase of any new IoT devices and the network connectivity for any existing IoT devices.
3. Any exception to the Policy due to specific business, security or technical requirements or constraints must be approved by the Chief Information Officer (CIO).
4. Violation of the Policy may result in restrictions on IT network, application or service access in addition to administrative and/or disciplinary actions outlined in the other relevant College policies.

## **DEFINITIONS**

Internet of Things (IoT) device: Any device, which is able to connect to a wired or wireless computer network and which is not a computer, tablet or smartphone. Examples of IoT device are smart TVs, digital whiteboards, remotely controlled HVAC systems, remotely controlled refrigerators, IP and network enabled cameras, audio and video streaming devices, etc.

## **RELATED LEGISLATION & POLICIES**

### Legislation

Freedom of Information and Protection of Privacy Act

### Policies

- A.3.6 Standards of Employee Conduct & Conflict of Interest
- B.4.1 Purchasing
- B.5.1 Sharing & Stewardship of Information
- B.5.2 Appropriate and Responsible Use of Educational and Information Technology

## **RELATED PROCEDURES**

Refer to B.5.5 Internet of Things Procedure.