RESOURCE INF-017G

Internet-of-Things Guideline

Purpose

The purpose of this guideline is to establish a defined IoT structure at Coast Mountain College (CMTN) to ensure that data and operations are properly secured.

Overview

IoT devices may be business-oriented, consumer-based, or a hybrid of both. The devices may be company-provided or employee-owned, such as through a BYOD arrangement.

Definitions

Data Point: A discrete unit of information. Any single fact is a data point.

Internet of Things (IoT): Network- or Internet-connected devices such as appliances, thermostats, monitors, sensors, and portable items that can measure, store, and transmit information. The IoT connects billions of devices to the Internet and involves the use of billions of data points, all of which need to be secured.

Scope

IoT devices continue making inroads in the business world; therefore, it is necessary for CMTN to have this structure in place.

Details

IoT Device Procurement

IoT devices that are to be used for CMTN operations should be purchased and installed by IT personnel.

Employee-owned IoT devices used for business purposes must be used in accordance with INF-023G, *Personal Device Acceptable Use and Security Guideline*.

The use of all IoT devices, whether provided by CMTN or employee owned, should be requested via Appendix A*, IoT Device Usage Request Form* and submitted to the IT department for approval. Only manager-level employees and above may request the usage and/or procurement of IoT devices.

The IT department is responsible for identifying compatible platforms, purchasing equipment, and supporting CMTN-provided and authorized IoT devices.

Cybersecurity Risks and Privacy Risk Considerations

It is important for CMTN staff to understand the use of IoT because many IoT devices affect cybersecurity and privacy risks differently than IT devices do. Being aware of the existing IoT usage and possible future usage will assist CMTN in understanding how the characteristics of IoT affect managing cybersecurity and privacy risks, especially in terms of risk response.

It is important for CMTN to manage cybersecurity and privacy risk for IoT devices versus conventional IT devices, determining how those risk considerations might impact risk management in general, risk response and particularly mitigation, and identifying basic cybersecurity and privacy controls the College may want to consider, adapt, and potentially include in requirements when acquiring IoT devices.

The *IoT Risk Management Guide* contains insight as to the differences in risk between conventional IT devices and IoT devices. This document resides in the IT document storage area.

Related Policies, Guidelines and Other Resources

- INF-023G, *Personal Device Acceptable Use and Security Guideline*

Appendix A: IoT Device Usage Request Form

_____
Date

_____
Manager's Name

_____
Type of Device

_____
Date Needed

Describe the need for this device: