# CyberSecure Introduction

*The Road to Certification*

CyberSecure Fleming Group Project Winter 2023

Prof Mamdouh Mina, Computer Security & Investigation

# Welcome to CyberSecure!

The field of cyber security is the ever-evolving study of electronic threats and risks. These threats and risks can come from everywhere we expect, or from places we had never considered… until it is too late.

Because of this, businesses need a way to show users that their data is secure. A way to set themselves apart from those that simply *say* they are secure, and expect us to trust them.

This is where CyberSecure comes in. By applying a strong standard of safety through CyberSecure certification, an organization is able to show that they are prepared for whatever threats arise.

Like most things in life, the first step is admitting a problem is there. By beginning to learn about this process, your organization is showing what so many other Canadian companies already know; cyber security is paramount to a healthy business model.

# Before We Begin

The guides and examples you are about to read are meant to cover the basics of what will be required to work towards CyberSecure certification. There is no guarantee that using these specific examples will mean a positive outcome. Also, feel free to change these pages as your company sees fit. There is no "one size fits all" when it comes to such a changing field.

There are free learning modules available on https://ised-isde.canada.ca/site/cybersecure-canada/en/elearning. It is strongly suggested to go through these, starting with Introduction to certification.

The examples are on the accompanying Excel document. They are by no means exhaustive, but will still show a solid foundation for your business to begin this process.

# REVISION HISTORY

As with any documentation regarding processes, changes will have to be made as threats evolve, new assets arrive, and new thinking emerges. It is considered best practice that such policies and procedures are updated in a regular fashion.

## IT Hardware Inventory

Keeping track of physical computer assets is the first step towards a strong cyber security posture. Knowing what is on hand means having control over portals of infection for the organization.

*There exists software that can be purchased that will keep track of assets. Such software, or even paper documentation, is acceptable for CyberSecure purposes.

## IT Software Inventory

Software is where computers meet people. Just as with hardware, knowing what software should be running internally means making it easy to know what software should be present, and which shouldn't.

*There exists software that can be purchased that will keep track of assets. Such software, or even paper documentation, is acceptable for CyberSecure purposes.

## General Security Controls and Justifications

This portion is for listing what plans, processes, procedures exist already, as well as the reasons for them. This could be done in a simple list format.

# Asset Security

Each asset will have to be grouped together with like/similar assets. Each one will have to follow a consistent process in order to be found in compliance with CyberSecure. For example; if one desktop is set up to require a password, all desktops should require that as well.

The chart below is an example of what a standard of security could look like. Again, make changes as your organization sees fit.

| Criticality | User Auth | Auto Patching | Remote Mgmt | Wi-fi | Blue Tooth | Shared Drive | Storage Encrypt | Onsite Backup | Offsite Backup | Perimeter Defense |
|---|---|---|---|---|---|---|---|---|---|---|
| Backup and encrypt data | Use strong user authentication | Automatically patch operating systems and applications | Establish basic perimeter defences | Securely configure devices<br>Secure mobility<br>Establish basic perimeter defences | Securely configure devices | Implement access control and authorization | Securely configure devices<br>Backup and encrypt<br>Secure portable media | Backup and encrypt data | Backup and encrypt data | Establish basic perimeter defences |