[Insert Organization Name]

Digital Asset Catalogue

**Disclaimer**

**Instructions:** CyberSecure Canada has developed this template for your use in relation to certification requirements for the eLearning series. It provides guidance as to how information can be organized and documented for certification. CyberSecure Canada does not guarantee a successful certification from use of this template. Organizations are not obliged to use this template and may provide the certification requirement(s) in a documented format best suited for them.

Template Instructions

**Instructions:** Instructions are provided in blue font within each section of this template. Upon completion of the template, delete these instructions.

It is recommended that users review the eLearning module for **Introduction to Certification** and the completed example of a Digital Catalogue.

This template is prepared for and by the CyberSecure Canada certification program to help organizations develop the various policies, documentation and inventories required to meet the certification requirements of CyberSecure Canada. **Instructions end.**

Revision history

**Instructions:** It is a best practice for organizations to ensure their policies are reviewed and updated regularly. Document what changes are made, when, and by whom.

The Digital Asset Catalogue has been modified as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Modification | Modifier |
| [Date edited] | [Document version] | [Description of changes made] | [Name of the editor] |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

General Security Controls & Justifications

**Instructions:**

* List the security control features that your organization has decided to implement universally on its hardware and software assets.
  + For example: Automatic Patching – We have standardized enabling automatic patching wherever possible across our organization. This is to reduce the risk of malware.

[Insert Company Name] has reviewed the devices and implemented the following security controls universally:

* [Insert security feature and description]
* [Insert security feature and description]
* [Insert security feature and description]
* [Insert security feature and description]

Inventory of assets

**Instructions:**

* The Digital Asset Catalogue must consist of all your organization’s digital assets including both hardware and software. This catalogue is foundational and is an inventory of all your organization’s digital assets. It contains other required information for each of these assets that will be needed to comply with certification requirements.
* Please note that the Inventory table is not the only method to catalogue the necessary information. Software that can will track your hardware and software inventory is also available for purchase at the discretion of your organization. Organizations are encouraged to determine the best approach for their own needs.
* To begin completing the inventories below, organizations must take the following steps:

**Step 1:** List the hardware and software used in your organization (the first seven columns of the inventory table)

**Step 2:** Using the list of hardware and software assets from step 1, complete the other columns in the table. The information required for the “Security Controls and Justification” columns form part of the certification requirements for each security control area.

* + - The table below outlines which security control areas are relevant to that specific column and the title of the module in this eLearning series where you can find more information on this topic.
    - As you progress through the certification requirements, you are encouraged to update this catalogue to reflect action/decisions taken.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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    Secure Mobility  Establish Basic Perimeter Defences | Securely Configure Devices | Implement Access Control and Authorization | Securely Configure Devices  Backup and Encrypt  Secure Portable Media | Backup and Encrypt Data | Backup and Encrypt Data | Establish Basic Perimeter Defences |

IT Hardware Inventory

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | **Device Type** | **Vendor** | **Model** | **Assignee** | **O/S** | **Purchase Date** | **Security Controls And Justifications** | | | | | | | | | | | |
|  |  |  |  |  |  |  | Criticality | User  Auth | Auto  Patching | Remote  Mgmt | Wi-Fi | Blue  Tooth | Shared  Drive | Storage  Encrypt | Onsite  Backup | Offsite  Backup | Offline Backup | Perimeter  Defense |
| 1 | Laptop | Dell | Latitude 7410 Standard | John Doe | Windows 10 | 2020-03-01 | 1-Critical Can operate for two days without. Workaround: close temporarily. | 2FA Standard | Auto  Standard | Disabled  Standard | Enabled  Standard | Disabled Standard | \\NAS\Exec Executive use | Yes Standard | \\NAS\Backup Nightly | OneDrive  Standard | Western Digital HDD  Monthly | Windows Firewall Standard |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

IT Software Inventory

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | **Vendor** | **Software**  **& Version** | **Technical**  **Owner** | **Update**  **Method** | **Installed**  **On** | **Confidential**  **Info Stored** | **Security Controls And Justifications** | | | | | | | |
|  |  |  |  |  |  |  | Criticality | Hardening Guide | Auto  Patching | Remote Mgmt | User  Auth | Onsite  Backup | Offsite  Backup | Offline Backup |
| 1 | Intuit | Quickbooks Payroll | John Doe | Auto | Cloud | Yes-SIN | 1-Critical Can operate for two days without. Workaround: don’t run payroll for the time being. | n/a | Auto Standard | n/1 | Microsoft SSO  2FA | \\NAS\Backup  Nightly | OneDrive  Standard | Western Digital HDD  Monthly |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |