IT Asset Security Hardening Policy

Table of Contents

[Background 2](#_Toc17192145)

[Purpose 3](#_Toc17192146)

[Definitions 3](#_Toc17192147)

[IT Asset Security Hardening Management Policy 3](#_Toc17192148)

[Responsibilities 4](#_Toc17192149)

# Background

**[Describe The Background Of Why An IT Asset Security Hardening Policy Has Come About.]**

The **[Business Name]** acknowledges the need to protect and manage its information technology (IT) assets and therefore, the **[Business Name]** is establishing this IT Asset Security Hardening Policy to implement a systematic process to strengthen the security of servers and operating systems to improve **[Business Name]** overall security posture.

# Purpose

**[Describe What The Intent Of This Document Will Be.]**

This document sets forth the Policy for **[Business Name]**. It establishes the business rules and

guidelines for consistency and compliance in executing the **[Business Name]** IT Asset Security Hardening Policy process and procedures for protecting and managing IT assets.

# Definitions

**[Define Any Terms That Are Used Throughout This Document.]**

|  |  |
| --- | --- |
| Terms | Definition |
| IT Asset | **IT Asset** refers to anything (tangible or intangible) that has value to an organisation, including, but not limited to, a computing device, IT system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualised computing), and related hardware (e.g., locks, cabinets, keyboards), as well as people and intellectual property (including software). |
|  |  |

# IT Asset Security Hardening Management Policy

**[Describe The Rules That Govern The Policy]**

All [Business Name] IT assets shall be managed in accordance with all Government mandates, and **[Business Name]** policy and procedures. This policy establishes the business rules and guidelines below for hardening IT Security Assets.

The **[Business Name]** shall:

* A server/workstation must not be connected to the **[Business Name]** production network until it is in an approved secure state.
* The Hardening Procedure follows the CIS Benchmarks for each Operating System (Windows & Linux) and is required to harden an operating system and must be implemented prior to approval. Steps included:
	+ The CIS Hardening Benchmark Hardening Document Is Followed & Implemented
	+ Applying All Vendor Supplied Patches And Updates
	+ Removal Of Unnecessary Software, Services And Ports
	+ Backup Agent Installed And Added To Backup Schedule (Where Applicable)
	+ EndPoint Protection Software Has Been Installed And Is Updated.
	+ Asset Is Added To Vulnerability Scan Scope
	+ Disable Or Changing Default User Accounts
	+ Changing Default Passwords
	+ Log Are Configured To Be Captured As Per The Audit And Logging Plan
	+ Applying Domain Based Groups And Policies

**[Add In More Steps Where Appropriate]**

# Responsibilities

**[List Who Is Responsible For Adhering To The Policy]**

**Responsibilities For IT Administrators**

* Develop process, and procedures to include automated, repeatable processes to improve efficiency and reliability