Privileged Access Policy

Table of Contents

[Background 3](#_Toc16768998)

[Purpose 3](#_Toc16768999)

[Definitions 3](#_Toc16769000)

[IT Asset Management Policy 4](#_Toc16769001)

[Responsibilities 5](#_Toc16769002)

[IT Asset Lifecycle Management Overview 5](#_Toc16769003)

[Plan 6](#_Toc16769004)

[Aquire 6](#_Toc16769005)

[Deploy 6](#_Toc16769006)

[Manage 7](#_Toc16769007)

[Dispose 7](#_Toc16769008)

# Background

**[Describe The Background Of Why A Privileged Access Policy Has Come About.]**

The **[Business Name]** acknowledges the need to manage privileged access to its information technology (IT) assets and therefore, the **[Business Name]** is establishing this Privileged Access Policy to implement a systematic process that reduces the risk of unauthorised access using privileged credentials by limiting access to only those individuals that require privileged access to **[Business Name]** IT systems.

# Purpose

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

This document sets forth the Privileged Access Policy for **[Business Name]**. It establishes the business rules and guidelines for consistency and compliance in executing the **[Business Name]** Privileged Access process and procedures for managing access to 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). |
| Privileged Access: | Privileged Access: Access that allows an individual who can take actions which may affect computing systems, network communication, or the accounts, files, data or processes of other users.  Privileged access is typically granted to system administrators, network administrators or other such employees whose job duties require access to sensitive data residing on a system or network.  This data can be paper or electronic data. For the purposes of this policy, application and other developers are also considered privileged. |

# Privileged Access Policy

**[Describe The Details Of 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 managing Privileged Access to IT assets.

The **[Business Name]** shall:

* Privileged Access users must use individual accounts with unique user names and passwords that comply with the **[Business Name]** Password Policy.
* If there is a business need for shared credentials (e.g. Service Accounts), an approved password storage system must be used. Access to the password storage system must be controlled by the **[Business Name]** approved multi-factor authentication system.
* The Principle of Least Privilege must be followed. Privileged Access users must have access set to the lowest level of access needed to accomplish their job function.
* The Appropriate **[Business Name]** system ownerand ITmust approve all Privileged Access accounts and review all users with Privileged Access monthly to determine if Privileged Access is still needed and to review what level of access is appropriate.
* Privileged Access users should only have access on a Need to Know basis. The users should only have access to, and knowledge of, only the data needed to do their job function.
* It is the responsibility of each system owner or business unit, to utilise a Separation of Duties and Rotation of Duties plan.
* Regular review of system logs is required to monitor Privileged Access user accounts for misuse.
* Appropriate logs must be maintained in a centralised system where integrity and access can be controlled.
* Privileged Access users’ desktop or laptop computers must be **[Business Name]** owned and must be managed by **[Business Name]**
* Individuals with Privileged Access must respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with all relevant laws, policies and procedures.
* Privileged Access use must be reserved for tasks that require the use of Privileged Access. If methods other than using Privileged Access will accomplish a task, those other methods must be used.

# Responsibilities

**[List Who Is Responsible For Sponsoring, Setting Up And Maintaining The Program.]**

**Responsibilities For Privileged Access Users**

Privileged Access users shall take necessary precautions to protect the confidentiality and integrity of information encountered in the performance of their duties. If, during the performance of their duties, users observe strange activity or evidence indicating misuse, they must immediately notify their supervisor and IT Security.