BUSINESS REQUIREMENT DOCUMENT

Local Administrator Password Solution (LAPS)

Document Information

|  |  |
| --- | --- |
| Document Attributes | Description |
| Document ID | Doc001 |
| Author | Sandeep Taksande |
| Contributor | - |

Revision History

|  |  |  |
| --- | --- | --- |
| Version | Date | Changes |
| Draft | 01-October-2024 | New Document |
| V0.1 |  |  |
|  |  |  |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewer/ Approver | Role | Comments | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1. Introduction 4](#_Toc179291738)

[1.1 Purpose 4](#_Toc179291739)

[1.2 Scope 4](#_Toc179291740)

[2. Business Objectives 4](#_Toc179291741)

[3. As-Is Situation 4](#_Toc179291742)

[4. To-Be Situation 4](#_Toc179291743)

[5. Key Stakeholders 4](#_Toc179291744)

[6. Project Constraints 5](#_Toc179291745)

[7. Cost-Benefit Analysis 5](#_Toc179291746)

[8. Functional Requirements 5](#_Toc179291747)

[9. Success Criteria 6](#_Toc179291748)

# 1. Introduction

## 1.1 Purpose

The purpose of this BRD is to define the business requirements for implementing Microsoft LAPS within our organization. LAPS is a tool designed to centrally manage and rotate local administrator passwords on Windows domain-joined computers. This will enhance security by reducing the risk of unauthorized access and password compromise.

## 1.2 Scope

This BRD covers the implementation of LAPS for all Windows domain-joined computers within our organization. It includes the configuration of LAPS policies, password rotation schedules, and integration with Active Directory.

# 2. Business Objectives

The primary business objectives of implementing LAPS are:

* **Enhance security:** Reduce the risk of unauthorized access to critical systems by implementing strong password management practices.
* **Improve compliance:** Ensure compliance with industry regulations and best practices for password management.
* **Reduce administrative overhead:** Streamline the process of managing local administrator passwords.
* **Increase operational efficiency:** Improve the overall security posture of the organization.

# 3. As-Is Situation

Currently, local administrator passwords are managed manually, leading to inconsistent practices and potential security risks. There is no centralized control over password complexity, rotation, or expiration.

# 4. To-Be Situation

After LAPS implementation, local administrator passwords will be centrally managed and rotated according to defined policies. Password complexity, expiration, and rotation schedules will be enforced, ensuring a higher level of security.

# 5. Key Stakeholders

The following key stakeholders are involved in this project:

* **IT Department:** Responsible for the technical implementation and management of LAPS.
* **Security Team:** Responsible for defining security policies and ensuring compliance.
* **End-users:** May be impacted by changes to password management procedures.

# 6. Project Constraints

The following project constraints should be considered:

* **Budget:** The project must be completed within the allocated budget.
* **Timeline:** The project must be completed within the specified timeframe.
* **Resources:** The project team must have the necessary resources (skills, tools, etc.) to complete the implementation.

# 7. Cost-Benefit Analysis

The cost-benefit analysis for LAPS implementation includes:

* **Costs:**
  + Hardware and software costs associated with LAPS deployment.
  + Training costs for IT staff.
  + Administrative overhead associated with managing LAPS.
* **Benefits:**
  + Reduced risk of unauthorized access and data breaches.
  + Improved compliance with industry regulations.
  + Increased operational efficiency.
  + Reduced administrative overhead.

# 8. Functional Requirements

The functional requirements for LAPS implementation include:

* **Centralized password management:** LAPS must provide a centralized mechanism for managing local administrator passwords.
* **Password rotation:** LAPS must enforce regular password rotation schedules.
* **Password complexity:** LAPS must enforce strong password complexity requirements.
* **Password expiration:** LAPS must enforce password expiration policies.
* **Integration with Active Directory:** LAPS must integrate seamlessly with Active Directory.
* **Reporting and auditing:** LAPS must provide detailed reporting and auditing capabilities.

# 9. Success Criteria

The success criteria for LAPS implementation include:

* **Successful deployment:** LAPS must be successfully deployed and configured in the organization.
* **Adherence to policies:** Local administrator passwords must be managed and rotated according to defined policies.
* **Reduced security incidents:** The number of security incidents related to unauthorized access should decrease after LAPS implementation.
* **Improved compliance:** The organization should be able to demonstrate compliance with industry regulations and best practices for password management.
* **User satisfaction:** End-users should be satisfied with the new password management procedures.