BUSINESS REQUIREMENT DOCUMENT

Bitlocker

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](#_Toc179896755)

[1.1 Purpose 4](#_Toc179896756)

[1.2 Scope 4](#_Toc179896757)

[2. Business Objectives 4](#_Toc179896758)

[3. As-Is Situation 4](#_Toc179896759)

[4. To-Be Situation 4](#_Toc179896760)

[5. Key Stakeholders 4](#_Toc179896761)

[6. Project Constraints 5](#_Toc179896762)

[7. Cost-Benefit Analysis 5](#_Toc179896763)

[8. Functional Requirements 5](#_Toc179896764)

[9. Success Criteria 6](#_Toc179896765)

# 1. Introduction

## 1.1 Purpose

This document outlines the business requirements for implementing BitLocker encryption on corporate devices to enhance data security and compliance. BitLocker will be used to encrypt hard drives and removable storage devices, protecting sensitive data from unauthorized access.

## 1.2 Scope

**T**he scope of this project includes the implementation of BitLocker encryption on all corporate-owned devices, including laptops, desktops, and servers. It will cover the configuration of BitLocker policies, user training, and ongoing management of the encryption solution.

## 2. Business Objectives

* **Data Security:** Protect sensitive data from unauthorized access, theft, and loss.
* **Compliance:** Ensure compliance with industry regulations and internal data security standards.
* **Risk Mitigation:** Reduce the risk of data breaches and financial losses.
* **Operational Efficiency:** Streamline the management of data security measures.

## 3. As-Is Situation

Currently, the organization does not have a standardized encryption solution in place. Data is at risk of unauthorized access and potential breaches.

## 4. To-Be Situation

After the implementation of BitLocker, all corporate devices will be equipped with robust encryption capabilities. Sensitive data will be protected, reducing the risk of data breaches and improving overall data security posture.

## 5. Key Stakeholders

* **IT Department:** Responsible for the technical implementation and management of BitLocker.
* **Security Team:** Oversees data security policies and procedures.
* **Legal Department:** Ensures compliance with relevant regulations and standards.
* **End-Users:** Will be impacted by the encryption process and may require training.

## 6. Project Constraints

* **Budget:** The project must adhere to the allocated budget for hardware, software, and implementation costs.
* **Timeline:** The implementation must be completed within a specified timeframe to meet business objectives.
* **Compatibility:** BitLocker must be compatible with existing hardware and software infrastructure.

## 7. Cost-Benefit Analysis

**Benefits:**

* Reduced risk of data breaches and associated costs.
* Improved data security posture.
* Enhanced compliance with industry regulations.
* Potential cost savings from reduced insurance premiums.

**Costs:**

* Hardware and software costs associated with BitLocker implementation.
* Training costs for end-users and IT staff.
* Ongoing management and maintenance costs.

**Net Benefits:** The net benefits of implementing BitLocker will depend on the specific costs and benefits associated with the project. However, the potential reduction in risk and improved security posture can outweigh the initial costs.

## 8. Functional Requirements

* **Encryption:** BitLocker must be configured to encrypt all hard drives and removable storage devices on corporate devices.
* **Authentication:** Users must authenticate using strong passwords or other approved methods to unlock encrypted data.
* **Key Management:** BitLocker must securely manage encryption keys to prevent unauthorized access.
* **Policy Enforcement:** BitLocker policies must be enforced to ensure consistent encryption practices across the organization.
* **Reporting:** BitLocker must provide reports on encryption status, compliance, and potential issues.

## 9. Success Criteria

* **Encryption Coverage:** All corporate devices must be successfully encrypted.
* **Compliance:** The organization must be in compliance with relevant data security regulations and standards.
* **User Adoption:** End-users must be trained and able to effectively use BitLocker.
* **Security Incidents:** The number of data security incidents must be reduced after BitLocker implementation.
* **Cost-Effectiveness:** The project must be completed within the allocated budget and deliver the expected benefits.