FUNCTIONAL REQUIREMENT DOCUMENT

Microsoft 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](#_Toc179896935)

[1.1 Purpose 4](#_Toc179896936)

[1.2 Scope 4](#_Toc179896937)

[**2.** Functional Requirements 4](#_Toc179896938)

[2.1. Encryption 4](#_Toc179896939)

[2.2 Authentication 4](#_Toc179896940)

[2.3 Key Management 5](#_Toc179896941)

[2.4 Policy Enforcement 5](#_Toc179896942)

[2.5 Reporting 5](#_Toc179896943)

[2.6 Integration 6](#_Toc179896944)

[2.7 User Experience 6](#_Toc179896945)

[2.8 Additional Considerations 6](#_Toc179896946)

[3. Non-Functional Requirements 6](#_Toc179896947)

[3.1 Performance 6](#_Toc179896948)

[3.2 Scalability 7](#_Toc179896949)

[3.3 Availability 7](#_Toc179896950)

[3.4 Security 7](#_Toc179896951)

[3.5 Reliability 7](#_Toc179896952)

[3.6 Usability 7](#_Toc179896953)

[3.7 Compatibility 8](#_Toc179896954)

[3.8 Maintainability 8](#_Toc179896955)

[3.9 Portability 8](#_Toc179896956)

# 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.** Functional Requirements

## 2.1. Encryption

* **Requirement:** All corporate-owned devices, including laptops, desktops, and servers, must be encrypted using BitLocker.
  + **Acceptance Criteria:**
    - 100% of devices are encrypted with BitLocker.
    - Encryption status can be verified through BitLocker management tools.
* **Requirement:** BitLocker must be configured to encrypt both fixed drives and removable storage devices.
  + **Acceptance Criteria:**
    - Encryption is enabled for both internal and external drives.
    - Removable storage devices are automatically encrypted when connected to the device.

## 2.2 Authentication

* **Requirement:** Users must authenticate using strong passwords or other approved methods to unlock encrypted data.
  + **Acceptance Criteria:**
    - Password requirements adhere to organizational security policies.
    - Users can use alternative authentication methods like smart cards or biometrics if supported.
* **Requirement:** BitLocker must support pre-boot authentication to prevent unauthorized access before the operating system loads.
  + **Acceptance Criteria:**
    - Pre-boot authentication is enabled by default.
    - Users can configure pre-boot authentication settings.

## 2.3 Key Management

* **Requirement:** BitLocker must securely manage encryption keys to prevent unauthorized access.
  + **Acceptance Criteria:**
    - Encryption keys are stored in a secure location.
    - Key recovery options are in place for lost or forgotten passwords.
* **Requirement:** BitLocker must support TPM-based hardware protection of encryption keys.
  + **Acceptance Criteria:**
    - TPM is enabled on supported devices.
    - Encryption keys are protected by the TPM.

## 2.4 Policy Enforcement

* **Requirement:** BitLocker policies must be enforced to ensure consistent encryption practices across the organization.
  + **Acceptance Criteria:**
    - Group Policy Objects (GPOs) or other management tools are used to enforce BitLocker policies.
    - Policies can be configured to set encryption requirements, authentication methods, and recovery options.
* **Requirement:** BitLocker must support compliance with industry regulations (e.g., HIPAA, GDPR).
  + **Acceptance Criteria:**
    - BitLocker configuration can be adjusted to meet specific regulatory requirements.
    - Compliance reports can be generated to demonstrate adherence to regulations.

## 2.5 Reporting

* **Requirement:** BitLocker must provide reports on encryption status, compliance, and potential issues.
  + **Acceptance Criteria:**
    - Reports can be generated on a regular basis.
    - Reports include information on encrypted devices, compliance status, and any security incidents.
    - Reports can be exported in various formats (e.g., CSV, PDF).

## 2.6 Integration

* **Requirement:** BitLocker must integrate with existing systems and tools (e.g., Active Directory, SIEM).
  + **Acceptance Criteria:**
    - BitLocker can be managed through Active Directory.
    - Security events can be logged in a SIEM for monitoring and analysis.

## 2.7 User Experience

* **Requirement:** The user experience for BitLocker must be intuitive and easy to understand.
  + **Acceptance Criteria:**
    - Clear and concise instructions are provided to users.
    - The BitLocker interface is user-friendly and accessible.
    - Users can easily access help and support resources.

## 2.8 Additional Considerations

* **Testing:** A comprehensive testing plan should be developed to ensure BitLocker functions as expected and meets all requirements. Testing should include unit testing, integration testing, system testing, and user acceptance testing.
* **Training:** Training materials and resources should be developed to educate users on BitLocker best practices and troubleshooting techniques.
* **Support:** A support process should be established to address user questions and issues related to BitLocker.

# 3. Non-Functional Requirements

## 3.1 Performance

* **Requirement:** BitLocker encryption and decryption processes must not significantly impact system performance.
  + **Acceptance Criteria:**
    - Encryption and decryption speeds are within acceptable limits for the targeted devices.
    - System responsiveness is not noticeably affected during encryption or decryption operations.

## 3.2 Scalability

* **Requirement:** BitLocker must be scalable to accommodate a growing number of devices and data volumes.
  + **Acceptance Criteria:**
    - BitLocker can efficiently manage encryption for a large number of devices.
    - Performance does not degrade significantly as the number of devices and data volumes increases.

## 3.3 Availability

* **Requirement:** BitLocker must have high availability and minimal downtime.
  + **Acceptance Criteria:**
    - BitLocker is resilient to hardware failures and system crashes.
    - Recovery procedures are in place to minimize downtime in case of issues.

## 3.4 Security

* **Requirement:** BitLocker must implement robust security measures to protect against unauthorized access and attacks.
  + **Acceptance Criteria:**
    - Encryption algorithms are strong and resistant to known attacks.
    - Key management practices are secure and compliant with industry standards.
    - BitLocker is regularly updated with security patches and fixes.

## 3.5 Reliability

* **Requirement:** BitLocker must be reliable and consistent in its operation.
  + **Acceptance Criteria:**
    - BitLocker functions as expected under various conditions and workloads.
    - Encryption and decryption operations are consistent and predictable.

## 3.6 Usability

* **Requirement:** BitLocker must be easy to use and manage for both end-users and administrators.
  + **Acceptance Criteria:**
    - The user interface is intuitive and easy to navigate.
    - Administrators can effectively manage BitLocker policies and settings.
    - Support resources are available to assist users and administrators.

## 3.7 Compatibility

* **Requirement:** BitLocker must be compatible with existing hardware, software, and operating systems.
  + **Acceptance Criteria:**
    - BitLocker is compatible with supported devices and operating systems.
    - BitLocker can integrate with existing security infrastructure and tools.

## 3.8 Maintainability

* **Requirement:** BitLocker must be easy to maintain and update.
  + **Acceptance Criteria:**
    - BitLocker can be updated with new features and security patches without significant disruption.
    - Maintenance tasks are manageable and efficient.

## 3.9 Portability

* **Requirement:** BitLocker must be portable and compatible with different hardware platforms.
  + **Acceptance Criteria:**
    - BitLocker can be deployed on various hardware platforms and operating systems.
    - Encryption keys can be transferred between devices without issues.