STATEMENT OF WORK

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. Project Overview 5](#_Toc179289063)

[1.1 Project Objectives 5](#_Toc179289064)

[1.2 Scope of Work 5](#_Toc179289065)

[1.2.1 Assessment and Planning 5](#_Toc179289066)

[1.2.2 Installation and Configuration 5](#_Toc179289067)

[1.2.3 Integration with Existing Systems 6](#_Toc179289068)

[1.2.4 Policy Development and Implementation 6](#_Toc179289069)

[1.2.5 User Training and Support 6](#_Toc179289070)

[1.2.6 Testing and Deployment 6](#_Toc179289071)

[2. Roles and Responsibilities 7](#_Toc179289072)

[2.1 Customer Responsibilities 7](#_Toc179289073)

[2.2 Vendor Responsibilities 7](#_Toc179289074)

[3. Project Timeline 7](#_Toc179289075)

[3.1 Project Phases and Timeline 7](#_Toc179289076)

[4. Deliverables 8](#_Toc179289077)

[4.1 Project Documentation 8](#_Toc179289078)

[4.2 Technical Deliverables 8](#_Toc179289079)

[4.3 Additional Deliverables (if applicable) 8](#_Toc179289080)

[5. Technical Requirements 8](#_Toc179289081)

[5.1 Hardware Requirements 8](#_Toc179289082)

[5.2 Software Requirements 8](#_Toc179289083)

[5.3 Network Requirements 9](#_Toc179289084)

[5.4 Security Requirements 9](#_Toc179289085)

[5.5 Compliance Requirements 9](#_Toc179289086)

[6. Implementation Methodology 9](#_Toc179289087)

[6.1 Assessment and Planning 9](#_Toc179289088)

[6.2 Installation and Configuration 10](#_Toc179289089)

[6.3 Integration with Existing Systems 10](#_Toc179289090)

[6.4 Policy Development and Implementation 10](#_Toc179289091)

[6.5 User Training and Support 10](#_Toc179289092)

[6.6 Testing and Deployment 10](#_Toc179289093)

[6.7 Post-Deployment Support 11](#_Toc179289094)

[7. Support and Maintenance 11](#_Toc179289095)

[7.1 Support Services 11](#_Toc179289096)

[7.2 Maintenance Services 11](#_Toc179289097)

[8. Payment Terms 11](#_Toc179289098)

[8.1 Payment Schedule 11](#_Toc179289099)

[8.2 Payment Terms 11](#_Toc179289100)

[9. Intellectual Property 12](#_Toc179289101)

[9.1 Ownership 12](#_Toc179289102)

[9.2 Intellectual Property Rights 12](#_Toc179289103)

[9.3 Intellectual Property Disclosures 12](#_Toc179289104)

[10. Confidentiality 12](#_Toc179289105)

[10.1 Non-Disclosure Agreement 12](#_Toc179289106)

[10.2 Disclosure Restrictions 12](#_Toc179289107)

[10.3 Return of Confidential Information 13](#_Toc179289108)

[11. Dispute Resolution 13](#_Toc179289109)

[11.1 Dispute Resolution Mechanism 13](#_Toc179289110)

[11.2 Governing Law 13](#_Toc179289111)

[11.3 Attorneys' Fees 13](#_Toc179289112)

[11.4 Change Management 13](#_Toc179289113)

# 1. Project Overview

## 1.1 Project Objectives

* **To implement Microsoft BitLocker to encrypt data at rest on client devices within the organization.** This will help protect sensitive data from unauthorized access, theft, or loss.
* **To enhance data security and compliance with industry regulations.** BitLocker can help organizations meet compliance requirements such as GDPR, HIPAA, and PCI DSS.
* **To protect sensitive data from unauthorized access, theft, or loss.** By encrypting data at rest, BitLocker can prevent unauthorized access even if devices are lost or stolen.
* **To provide a secure solution for storing and transmitting confidential information.** BitLocker can help ensure that confidential information remains secure, even when stored on external devices or transmitted over networks.

## 1.2 Scope of Work

### 1.2.1 Assessment and Planning

* **Conduct a comprehensive assessment of the existing IT infrastructure.** This will involve evaluating hardware, software, and network components to identify potential compatibility issues and risks.
* **Identify potential compatibility issues and risks associated with BitLocker implementation.** This will help ensure a smooth and successful deployment.
* **Develop a detailed project plan outlining the scope, timeline, resources, and deliverables.** This will provide a clear roadmap for the project and help manage expectations.
* **Assess the organization's readiness for BitLocker deployment, including security policies, user training, and support infrastructure.** This will help ensure that the organization has the necessary resources and processes in place to support BitLocker implementation.

### 1.2.2 Installation and Configuration

* **Install BitLocker on all eligible client devices within the organization.** This will involve installing the BitLocker software and configuring it to meet the organization's specific requirements.
* **Configure BitLocker settings according to the organization's security policies and requirements.** This will ensure that BitLocker is configured to provide the desired level of security.
* **Implement appropriate recovery options, such as recovery keys or TPM-based recovery.** This will help ensure that data can be recovered in case the encryption key is lost or compromised.
* **Configure BitLocker to integrate with existing authentication mechanisms (e.g., Active Directory, Azure AD).** This will allow BitLocker to leverage existing authentication methods and simplify user management.

### 1.2.3 Integration with Existing Systems

* **Integrate BitLocker with existing security systems, such as firewalls, intrusion detection systems, and antivirus solutions.** This will help ensure that BitLocker works seamlessly with other security measures.
* **Ensure compatibility with other data protection technologies (e.g., backup solutions, encryption-in-transit).** This will help prevent data loss and ensure that data is protected throughout its lifecycle.

### 1.2.4 Policy Development and Implementation

* **Develop and implement comprehensive BitLocker policies to govern the encryption of data at rest.** This will provide clear guidelines for BitLocker usage and help ensure compliance with industry regulations.
* **Define encryption requirements, recovery procedures, and compliance standards.** This will help ensure that BitLocker is used effectively and in accordance with best practices.
* **Establish roles and responsibilities for BitLocker management and administration.** This will help ensure that BitLocker is managed and maintained effectively.

### 1.2.5 User Training and Support

* **Develop and deliver user training programs to educate employees on BitLocker usage, recovery procedures, and security best practices.** This will help ensure that users understand how to use BitLocker effectively and safely.
* **Provide ongoing support and assistance to users regarding BitLocker-related issues.** This will help ensure that users can get the help they need to use BitLocker effectively.

### 1.2.6 Testing and Deployment

* **Conduct thorough testing of BitLocker implementation to ensure functionality and compatibility.** This will help identify and address any issues before BitLocker is deployed to the entire organization.
* **Perform pilot deployments to validate the solution and identify any issues.** This will help ensure that BitLocker is ready for full deployment and that any necessary adjustments can be made.
* **Roll out BitLocker to the entire organization in a phased manner.** This will help minimize disruption and ensure a smooth deployment process.

# 2. Roles and Responsibilities

## 2.1 Customer Responsibilities

* **Provide access to necessary systems and data for assessment and implementation.** This will allow the vendor to gather the information needed to plan and implement BitLocker.
* **Ensure compliance with applicable regulations and industry standards.** This will help ensure that BitLocker is implemented in a way that meets the organization's compliance requirements.
* **Provide adequate resources for user training and support.** This will help ensure that users are properly trained and supported, and that BitLocker is used effectively.
* **Review and approve project deliverables and milestones.** This will help ensure that the project is progressing according to plan and that the vendor is meeting the organization's expectations.

## 2.2 Vendor Responsibilities

* **Provide expert consulting services for BitLocker implementation.** This will involve providing guidance and expertise throughout the project.
* **Design, implement, and manage BitLocker solutions.** This will involve planning, installing, configuring, and managing BitLocker.
* **Ensure compliance with project objectives, timelines, and deliverables.** This will help ensure that the project is completed on time and within budget.
* **Provide ongoing support and maintenance services.** This will help ensure that BitLocker is running smoothly and that any issues are addressed promptly.

# 3. Project Timeline

## 3.1 Project Phases and Timeline

* **Phase 1: Assessment and Planning (4 weeks)**: This phase involves assessing the existing IT infrastructure, identifying potential risks, and developing a project plan.
* **Phase 2: Installation and Configuration (6 weeks)**: This phase involves installing BitLocker on client devices and configuring it according to the organization's requirements.
* **Phase 3: Integration and Testing (4 weeks)**: This phase involves integrating BitLocker with existing systems and conducting thorough testing.
* **Phase 4: Deployment and Training (4 weeks)**: This phase involves deploying BitLocker to the entire organization and providing user training.
* **Phase 5: Post-Deployment Support (2 weeks)**: This phase involves providing ongoing support and maintenance for BitLocker.

# 4. Deliverables

## 4.1 Project Documentation

* **Detailed project plan:** A comprehensive document outlining the scope, timeline, resources, and deliverables of the project.
* **Assessment report:** A report summarizing the findings of the assessment of the existing IT infrastructure.
* **BitLocker policy documentation:** A document outlining the organization's BitLocker policies and procedures.
* **User training materials:** Materials used to train users on BitLocker usage, recovery procedures, and security best practices.
* **Implementation report:** A report summarizing the key activities and outcomes of the BitLocker implementation project.

## 4.2 Technical Deliverables

* **BitLocker configuration files:** Files that define the BitLocker settings for the organization.
* **Recovery key management procedures:** Procedures for managing recovery keys to ensure that data can be recovered in case the encryption key is lost or compromised.
* **Integration scripts:** Scripts used to integrate BitLocker with other systems.
* **Test results:** Results of testing conducted to ensure that BitLocker is functioning properly and compatible with other systems.

## 4.3 Additional Deliverables (if applicable)

* **Custom scripts or tools:** Scripts or tools that may be developed to automate certain tasks or customize BitLocker.
* **Integration with third-party systems:** Integration with other systems, such as backup solutions or cloud storage providers.

# 5. Technical Requirements

## 5.1 Hardware Requirements

* **Compatible client devices (e.g., laptops, desktops):** BitLocker requires compatible hardware to function properly.
* **Sufficient storage capacity for encrypted data:** The devices must have enough storage space to accommodate the encrypted data.
* **Trusted Platform Module (TPM) for hardware-based encryption (recommended):** A TPM can provide additional security by storing encryption keys securely on the device.

## 5.2 Software Requirements

* **Microsoft Windows operating systems (supported versions):** BitLocker is only supported on certain versions of Windows.
* **Active Directory or Azure AD for authentication (if applicable):** BitLocker can be integrated with Active Directory or Azure AD to simplify user management.
* **Other relevant software (e.g., backup solutions, antivirus):** BitLocker may need to be integrated with other software to ensure comprehensive data protection.

## 5.3 Network Requirements

* **Network connectivity for BitLocker management and updates:** BitLocker requires network connectivity for management and updates.
* **Sufficient bandwidth for data encryption and decryption:** The network must have sufficient bandwidth to handle the data encryption and decryption process.

## 5.4 Security Requirements

* **Strong password policies:** Strong password policies should be in place to help protect against unauthorized access.
* **Regular security updates and patches:** All systems should be kept up-to-date with the latest security patches.
* **Data loss prevention measures:** Data loss prevention measures should be in place to help prevent accidental or intentional data loss.
* **Incident response procedures:** Incident response procedures should be in place to help respond to security incidents.

## 5.5 Compliance Requirements

* **Adherence to relevant industry standards (e.g., GDPR, HIPAA):** BitLocker can help organizations meet compliance requirements by protecting sensitive data.
* **Compliance with internal security policies:** BitLocker should be implemented in accordance with the organization's internal security policies.

# 6. Implementation Methodology

## 6.1 Assessment and Planning

* **Conduct a thorough assessment of the existing IT infrastructure.** This involves evaluating hardware, software, and network components to identify potential compatibility issues and risks.
* **Identify potential risks and challenges.** This includes assessing the organization's security posture, compliance requirements, and user readiness.
* **Develop a detailed project plan.** This outlines the scope, timeline, resources, and deliverables of the BitLocker implementation project.
* **Assess the organization's readiness for BitLocker deployment.** This involves evaluating the organization's security policies, user training, and support infrastructure.

## 6.2 Installation and Configuration

* **Install BitLocker on client devices.** This involves installing the BitLocker software on all eligible devices within the organization.
* **Configure BitLocker settings according to policies.** This involves configuring BitLocker to meet the organization's specific requirements, such as encryption mode, recovery options, and authentication methods.
* **Implement recovery options.** This involves setting up recovery keys or using TPM-based recovery to ensure that data can be recovered in case the encryption key is lost or compromised.
* **Integrate with existing systems.** This involves integrating BitLocker with other security systems and applications to ensure seamless operation.

## 6.3 Integration with Existing Systems

* **Integrate BitLocker with other security systems.** This includes integrating BitLocker with firewalls, intrusion detection systems, and antivirus solutions.
* **Ensure compatibility with other data protection technologies.** This involves ensuring that BitLocker works seamlessly with other data protection technologies, such as backup solutions and encryption-in-transit.

## 6.4 Policy Development and Implementation

* **Develop and implement BitLocker policies.** This involves creating comprehensive policies that govern the encryption of data at rest within the organization.
* **Define encryption requirements, recovery procedures, and compliance standards.** This involves specifying the types of data that should be encrypted, the recovery procedures that should be in place, and the compliance standards that need to be met.
* **Establish roles and responsibilities.** This involves assigning roles and responsibilities for BitLocker management and administration.

## 6.5 User Training and Support

* **Develop and deliver user training programs.** This involves creating and delivering training programs to educate users on BitLocker usage, recovery procedures, and security best practices.
* **Provide ongoing support and assistance.** This involves providing ongoing support and assistance to users regarding BitLocker-related issues.

## 6.6 Testing and Deployment

* **Conduct thorough testing.** This involves conducting various tests to ensure that BitLocker is functioning properly and compatible with other systems.
* **Perform pilot deployments.** This involves deploying BitLocker to a small group of users to test the solution in a controlled environment.
* **Roll out BitLocker to the entire organization.** This involves deploying BitLocker to all eligible devices within the organization.

## 6.7 Post-Deployment Support

* **Provide ongoing support and maintenance.** This involves providing ongoing support and assistance to users and administrators, as well as maintaining BitLocker and related components.
* **Monitor BitLocker performance and address any issues.** This involves monitoring BitLocker performance and addressing any issues that arise.

# 7. Support and Maintenance

## 7.1 Support Services

* **24/7 technical support for BitLocker-related issues.** This involves providing round-the-clock support for any BitLocker-related problems.
* **Remote troubleshooting and assistance.** This involves providing remote assistance to users and administrators to resolve BitLocker issues.
* **Incident management and resolution.** This involves managing and resolving security incidents related to BitLocker.

## 7.2 Maintenance Services

* **Regular updates and patches for BitLocker and related components.** This involves keeping BitLocker and related components up-to-date with the latest security patches and updates.
* **Performance monitoring and optimization.** This involves monitoring BitLocker performance and taking steps to optimize it.
* **Security vulnerability assessments and remediation.** This involves conducting regular security assessments and addressing any vulnerabilities that are identified.

# 8. Payment Terms

## 8.1 Payment Schedule

* **Milestone 1: Project Commencement (30% of total project cost)**: Payment is due upon signing of this Statement of Work.
* **Milestone 2: Completion of Installation and Configuration (50% of total project cost)**: Payment is due upon completion of the installation and configuration of BitLocker on all eligible devices.
* **Milestone 3: Final Project Delivery (20% of total project cost)**: Payment is due upon delivery of all project deliverables and successful completion of testing.

## 8.2 Payment Terms

* **Invoice Terms:** Invoices will be issued upon completion of each milestone. Payment is due within 30 days of the invoice date.
* **Late Payment Fees:** A late payment fee of 1.5% per month will be charged on any outstanding invoices after the due date.
* **Payment Methods:** Payments can be made by [specify acceptable payment methods, such as wire transfer, check, or credit card].

# 9. Intellectual Property

## 9.1 Ownership

* **Ownership of Intellectual Property:** All intellectual property rights created or developed during the course of this project, including but not limited to software, documentation, and any other materials, shall be owned solely by [Customer Name].

## 9.2 Intellectual Property Rights

* **Grant of License:** [Vendor Name] grants [Customer Name] a non-exclusive, worldwide, royalty-free license to use, reproduce, modify, distribute, and display the intellectual property created during the project for the purpose of implementing and operating BitLocker within [Customer Name]'s organization.
* **Restrictions:** [Vendor Name] retains ownership of all intellectual property rights not explicitly granted to [Customer Name] in this agreement. [Customer Name] shall not sublicense, assign, or transfer any of the rights granted to it under this agreement without the prior written consent of [Vendor Name].

## 9.3 Intellectual Property Disclosures

* **Disclosure of Intellectual Property:** If either party becomes aware of any actual or potential conflict between its intellectual property and the intellectual property of the other party, it shall promptly notify the other party. The parties shall cooperate in good faith to resolve any such conflicts.

# 10. Confidentiality

## 10.1 Non-Disclosure Agreement

* **Non-Disclosure Agreement:** Both parties agree to maintain the confidentiality of all Confidential Information disclosed to each other in connection with this agreement. Confidential Information includes any information that is designated as confidential or that should reasonably be considered confidential.

## 10.2 Disclosure Restrictions

* **Disclosure Restrictions:** Confidential Information shall not be disclosed to any third party without the prior written consent of the disclosing party, except as required by law or court order.
* **Permitted Disclosures:** Confidential Information may be disclosed to employees, contractors, or subcontractors of the receiving party who have a need to know such information for the purpose of performing their duties under this agreement. However, the receiving party shall ensure that such individuals are bound by confidentiality obligations similar to those contained in this agreement.

## 10.3 Return of Confidential Information

* **Return of Confidential Information:** Upon termination of this agreement or at the request of the disclosing party, the receiving party shall return or destroy all Confidential Information in its possession or control.
* **Retention of Confidential Information:** If required by law, the receiving party may retain a copy of Confidential Information for a period of time necessary to comply with legal or regulatory requirements.

# 11. Dispute Resolution

## 11.1 Dispute Resolution Mechanism

* **Mediation:** In the event of a dispute arising out of or in connection with this agreement, the parties shall first attempt to resolve the dispute through good faith mediation. A mutually agreed-upon mediator will be selected to facilitate the mediation process.

## 11.2 Governing Law

* **Governing Law:** This agreement shall be governed by and construed in accordance with the laws of the State of [State], without regard to its conflict of law principles.

## 11.3 Attorneys' Fees

* **Attorneys' Fees:** In the event of any litigation or arbitration arising out of or in connection with this agreement, the prevailing party shall be entitled to recover its reasonable attorneys' fees and costs.

## 11.4 Change Management

* **Change Management:** Any changes to this agreement shall be made in writing and signed by both parties. Any changes to the project scope, timeline, or deliverables shall be subject to a written change order, which shall specify the nature of the change, the impact on the project, and any adjustments to the contract price or schedule.