Company x

July 4, 2015

# IT Project Plan

## Project Overview

Due to recent security breaches across the nation, Company X has become increasingly concerned about protecting the contents of company computer hard drives. Currently, the company does have anti-virus software installed, data loss prevention, and malware protection on all workstations, but does not have any form of drive encryption. Without encryption, the data on computers could be stolen, hacked while offline, or viewed by unauthorized people.

As an encryption solution, Microsoft’s Bitlocker has been recommended. Bitlocker is a full disk encryption solution, which can be implemented by using technology that already exists on the company’s workstations. Something worth mentioning, this particular solution will contain a “free” or nearly free management solution. This is to forego the costs of $150 (per workstation) 3rd party solutions, and to not have to pay the $10 per seat by using MBAM and MDOP (Microsoft Bitlocker Reporting solutions). The project will have a budget for implementing Bitlocker, however, the TCO will be very low, while the ROI will be high, and continue to grow over time. When using this economical implementation method, companies can save hundreds of thousands of dollars (potentially millions of dollars) in Bitlocker implementation and management.

## Project Scope

The scope of the project includes implementing Bitlocker on all company workstations, some ten thousand computers. The time is set at six months, which includes development and testing, technical support for failed Bitlocker installations, replacing non-working machines with new, working computers, and training support staff.

## Project Budget

|  |  |  |
| --- | --- | --- |
| **Budget Item** | **Description** | **Finish** |
| 1.0 Project Start | Wed 7/1/15 | Fri 7/10/15 |
|  1.1 Create Project Overview | Wed 7/1/15 | Fri 7/3/15 |
|  1.2 Define Scope | Mon 7/6/15 | Wed 7/8/15 |
|  1.3 Define Business Plan | Mon 7/6/15 | Wed 7/8/15 |
|  1.4 Perform a Risk Assessment | Thu 7/9/15 | Fri 7/10/15 |
| 2.0 Project Planning | Sat 7/12/15 | Mon 1/6/14 |
|  2.1 Create Project Proposal |  |  |
|  2.2 Obtain Initial Approval from Stakeholders |  |  |

## Project Stakeholders

The stakeholders will include the CIO, CFO, the Change Management Team, the Senior Developer, and the Manager and Team Leader from the IT department.

|  |  |
| --- | --- |
| **Title** | **Description** |
| CFO | Chief Financial Officer, in charge of company finances |
| CIO | Chief Information Officer, in charge of company technology |
| Change Management Team | Authorizes changes to enterprise systems |
| Senior Developer | Responsible for software development |
| IT Manager | Communicates directly to IT staff |
| Team Leader | Performs training |

## Project Benefits

|  |  |
| --- | --- |
| **Benefit** | **Description** |
|  |  |
|  |  |
|  |  |

## Project ROI

The ROI has a few variables. One, standalone encryption software applications cost anywhere from $100-$200, so I will say $150 per workstation (that is $150 \* 10,000 workstations = $1,500,000) (Suneja, 2006). Next, the Microsoft reporting software costs $10 per seat, that is, 10 \* 10,000 workstations = $100,000. Adding these two figures together totals $1,600,000. The proposed solution costs $25,000 to implement.

## Project Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibility** |
|  |  |
|  |  |
|  |  |

## Project Work Breakdown Structure Project Dates: 07/1/2015-1/31/2016

|  |  |  |
| --- | --- | --- |
| **Task Name** | **Start** | **Finish** |
| 1.0 Project Start | Wed 7/1/15 | Fri 7/10/15 |
|  1.1 Create Project Overview | Wed 7/1/15 | Fri 7/3/15 |
|  1.2 Define Scope | Mon 7/6/15 | Wed 7/8/15 |
|  1.3 Define Business Plan | Mon 7/6/15 | Wed 7/8/15 |
|  1.4 Perform a Risk Assessment | Thu 7/9/15 | Fri 7/10/15 |
| 2.0 Project Planning | Sat 7/12/15 | Mon 1/6/14 |
|  2.1 Create Project Proposal |  |  |
|  2.2 Obtain Initial Approval from Stakeholders |  |  |
|  2.4 Create Budget |  |  |
|  2.5 Kickoff Meeting |  |  |
|  2.7 Identify Risks |  |  |
|  2.8 Create Contingency Plan for Risks |  |  |
|  2.9 Complete Business Analysis |  |  |
|  2.10 Draft Project Plan |  |  |
|  2.11 Draft Project Schedule |  |  |
|  2.12 Stakeholder Meeting for Design Approval |  |  |
| 3.0 Construction |  |  |
|  **3.1 Design** |  |  |
|  3.1.1 Coded Report for TPM status |  |  |
|  3.1.2 TPM Management for importing recovery keys |  |  |
|  3.1.2.1 Active Directory Import |  |  |
|  3.1.2.2 LANDesk Import |  |  |
|  3.1.2.3 Email Keys |  |  |
|  3.1.2.4 SFTP Keys |  |  |
|  3.1.3 Coded Reports for Bitlocker Status |  |  |
|  3.1.4 Stakeholder Meeting for Development Approval |  |  |
|  **3.2 Development** |  |  |
|  3.2.1 A coded report will be required for TPM status verification  |  |  |
|  3.2.2 Programming code to activate the TPM chip |  |  |
|  3.2.3 Programming code to take ownership of the TPM chip |  |  |
|  3.2.4 Programming code to add protectors to TPM chip |  |  |
|  3.2.5 Programming code to upload recovery keys to FTP server  |  |  |
|  3.2.6 Programming code to email recovery keys to service account |  |  |
|  3.2.7 Programming code to import rec. keys into Active Directory |  |  |
|  3.2.8 Programming code to import rec. keys into LANDesk/SCCM |  |  |
|  3.2.9 A coded report will be required for Bitlocker status |  |  |
|  3.2.10 All code successfully tested in lab environment |  |  |
|  **3.3 Software Unit Testing** |  |  |
|  3.3.1 Start Alpha Testing |  |  |
|  3.3.1.1 Identify software issues |  |  |
|  3.3.1.2 Fix software issues |  |  |
|  3.3.1.3 Test Again |  |  |
| 3.3.2 Start Beta Testing |  |  |
|  3.3.2.1 Identify software issues |  |  |
|  3.3.2.2 Fix software issues |  |  |
|  3.3.3.3 Test Again |  |  |
|  3.3.3 Prepare Report for Stakeholders |  |  |
|  3.3.4 Stakeholder Meeting for UaT Approval |  |  |
|  3.3.5 Complete Unit Testing |  |  |
|  **3.4 User Acceptance Testing** |  |  |
|  3.4.1 Start Pilot testing Group 1 Ohio Site |  |  |
|  3.4.1.1 Send emails to 5 users |  |  |
|  3.4.1.2 Enable TPM chips in Pilot Group |  |  |
|  3.4.1.3 Deploy TPM Management to Pilot Group |  |  |
|  3.4.1.4 Assess Users 1-5 in Pilot Group |  |  |
|  3.4.1.5 Address issues in hardware and/or software |  |  |
|  3.4.2 Start Pilot testing Group 1 Arizona Site |  |  |
|  3.4.2.1 Send emails to 5 users |  |  |
|  3.4.2.2 Enable TPM chips in Pilot Group |  |  |
|  3.4.2.3 Deploy TPM Management to Pilot Group |  |  |
|  3.4.2.4 Assess Users 1-5 in Pilot Group |  |  |
|  3.4.2.5 Address issues in hardware and/or software |  |  |
|  3.4.3 Start Pilot testing Group 1 Florida Site |  |  |
|  3.4.3.1 Send emails to 5 users |  |  |
|  3.4.3.2 Enable TPM chips in Pilot Group |  |  |
|  3.4.3.3 Deploy TPM Management to Pilot Group |  |  |
|  3.4.3.4 Assess Users 1-5 in Pilot Group |  |  |
|  3.4.3.5 Address issues in hardware and/or software |  |  |
|  3.4.4 Prepare report for Stakeholder meeting |  |  |
|  3.4.5 Stakeholder Meeting for Approval - Go-live approval |  |  |
|  3.4.6 User Acceptance Test Complete |  |  |
| 4.0 Implementation |  |  |
|  **4.1 Enable TPM Chips** |  |  |
|  4.1.1 Enable TPM Chips at Ohio site 3,300 computers |  |  |
|  4.1.1.1 Weekly Status Report (825 computers) |  |  |
|  4.1.1.2 Weekly Status Report (825 computers) |  |  |
|  4.1.1.3 Weekly Status Report (825 computers) |  |  |
|  4.1.1.4 Weekly Status Report (825 computers) |  |  |
|  4.1.2 Enable TPM Chips at Arizona site 3,300 computers |  |  |
|  4.1.2.1 Weekly Status Report (825 computers) |  |  |
|  4.1.2.2 Weekly Status Report (825 computers) |  |  |
|  4.1.2.3 Weekly Status Report (825 computers) |  |  |
|  4.1.2.4 Weekly Status Report (825 computers) |  |  |
|  4.1.3 Enable TPM Chips at Florida site 3,400 computers |  |  |
|  4.1.3.1 Weekly Status Report (850 computers) |  |  |
|  4.1.3.2 Weekly Status Report (850 computers) |  |  |
|  4.1.3.3 Weekly Status Report (850 computers) |  |  |
|  4.1.3.4 Weekly Status Report (850 computers) |  |  |
|  4.2 Create TPM Chip Master Status Report |  |  |
|  **4.3 Deploy TPM Management** |  |  |
|  4.3.1 Deploy TPM Management at Ohio site 3,300 computers |  |  |
|  4.3.1.1 Weekly Status Report (825 computers) |  |  |
|  4.3.1.2 Weekly Status Report (825 computers)  |  |  |
|  4.3.1.3 Weekly Status Report (825 computers) |  |  |
|  4.3.1.4 Weekly Status Report (825 computers) |  |  |
|  4.3.2 Deploy TPM Management at Arizona site 3,300 computers |  |  |
|  4.3.2.1 Weekly Status Report (825 computers) |  |  |
|  4.3.2.2 Weekly Status Report (825 computers) |  |  |
|  4.3.2.3 Weekly Status Report (825 computers) |  |  |
|  4.3.2.4 Weekly Status Report (825 computers) |  |  |
|  4.3.3 Deploy TPM Management at Florida site 3,400 computers |  |  |
|  4.3.3.1 Weekly Status Report (850 computers) |  |  |
|  4.3.3.2 Weekly Status Report (850 computers) |  |  |
|  4.3.3.3 Weekly Status Report (850 computers) |  |  |
|  4.3.3.4 Weekly Status Report (850 computers) |  |  |
|  4.1.4 Run TPM Management Status Report |  |  |
| 5.0 Project Closure |  |  |
|  5.1 Discuss Lessons Learned/Create PowerPoint |  |  |
|  5.2 Project Closure Report |  |  |
|  5.3 Close out project with Stakeholders |  |  |
|  5.4 Project Closure is Complete |  |  |

## Project Milestones

|  |  |
| --- | --- |
| **Milestone** | **Description** |
| Development | The first step in the Bitlocker rollout is to develop and test all the code that will be necessary to manage Bitlocker recovery keys. The deliverable will be code to report on TPM chips, code to manage the recovery keys, and code to report on Bitlocker compliance. |
| TPM Enable | Once all the code has been developed and tested, the next milestone will be to enable TPM chips on all workstations. This stage is critical to the overall process, because without the TPM being turned on, the recovery keys have no place to be stored. Now, there is a possible USB storage solution, however, to keep project costs (and TCO) low, the TPM chip has been selected as the best, cheapest recovery key storage option. This milestone will be complete when all TPM chips have been enabled. The deliverable will be a report stating the status of all TPM chips. |
| TPM Management | After the TPM chips have been enabled, the step stage of the process will be to collect Bitlocker recovery keys. Because I have chosen not to buy a Bitlocker management system, I will use code I have created to manage the retrieval and storage of Bitlocker recovery information. For this step, I will use SCCM or LANDesk (desktop management software) to deploy my TPM management scripted application. The TPM management does four things (1) Activates the TPM Chip, (2) takes ownership of the TPM, (3) adds protectors to the TPM, and (4) starts and pauses Bitlocker encryption. The deliverable for this milestone is a report verifying that TPM Management was indeed successful. |

## Project Risk Assessment

While Bitlocker is already built-in to most of Microsoft’s active operating systems, some problems may arise due to hardware or software failure. It is important to note, overall risks are very low because if the Bitlocker process does not work, in nearly 100% of the cases the user’s computer is fine to use; they just will not have Bitlocker. For the machines that Bitlocker was not installed, refer to the following chart.

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **Description** | **Mitigation** | **Role** |
| Failed TPM due to outdated BIOS | In rare cases, less than 1%, the computer’s BIOS may need to be updated to enable TPM. | BIOS will be manually updated. | Local Technician |
| Failed TPM due to motherboard | In rare cases, less than 1%, the computer’s motherboard will not have a TPM Chip. | Computer will be replaced with either a loaner machine or new computer. | Local Technician |
| Failed key import into Active Directory | The recovery key does not get imported into Active Directory | Try automated process again. Import key manually. | IT Specialist |
| Failed key import into Active Directory | The recovery key does not get imported into Active Directory | Verify computer is in a domain, and is in the proper OU.Or, enable, ‘Turn on TPM backup to Active Directory Domain Services’ in Local Group Policy | IT Specialist |
| Failed transport of key via email | The recovery key does not transport email service account | Try automated process again. Copy key from Active Directory, or FTP. Transfer manually. | IT Specialist |
| Failed transport of key to FTP server | The recovery key does not transport to FTP server | Try automated process again. Copy key from Active Directory or email. Transfer manually. | IT Specialist |
| Failed key import into LANDesk | The recovery key does not get imported into LANDesk Desktop Management Software | Reinstall LANDesk Agent. Try automated TPM Management. | Local Technician |
| User is receiving prompt to enter Bitlocker Recovery Password | When the user restarts their machine, they may receive a prompt to enter the Bitlocker Recovery Key | Enter the key from AD, FTP, Email, or LANDesk. Check TPM Chip status. Try automated TPM Management | IT Specialist |
| TPM cannot continue due to ownership error | The TPM ownership must be set before adding protectors to the TPM Chip | Take ownership of the TPM Chip, manually. Try automated TPM Management | IT Specialist |

# Approval and Authority to Proceed

We approve the project as described above, and authorize the team to proceed.

|  |  |  |
| --- | --- | --- |
| Name | Title | Date |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| Approved By |  |  | Date |  | Approved By |  |  | Date |