



# Enhancing Microsoft SharePoint Security

*How to improve collaboration while protecting information assets*

Whitepaper

April 2009

Information in this document is subject to change without notice. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written consent of Titus Labs Inc.

Titus Labs Inc. may have patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document.

© 2009 Titus Labs Inc.

Microsoft, Windows, Windows 2000, Windows XP, Windows Server 2003, Microsoft SharePoint Server, are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Titus Labs provides software classification solutions that make it possible for organizations to manage and control the flow of sensitive information inside and outside their enterprise in order to meet policy and compliance requirements.

For further information, contact us at (613) 820-5111 or email us at [info@titus.com](mailto:info@titus.com)  
<http://www.titus-labs.com/>

# Table of Contents

<i>Executive Summary</i> .....	4
<i>The Security Challenge in SharePoint</i> .....	4
<i>Risk #1 - Users obtain access to documents that they should not have access to</i> .....	5
<i>Risk #2 - Users download Office documents from SharePoint and then change them without authorization</i> .....	6
<i>Risk #3 - Users share documents that are not properly labeled for security and compliance</i> .....	6
<i>Addressing the Security Risks</i> .....	7
<i>What to Look For in a Solution</i> .....	10
<i>The Titus Labs Advantage</i> .....	11
• <i>Titus Labs Metadata Security for SharePoint</i> .....	11
• <i>Titus Labs PDF Control for SharePoint</i> .....	12
• <i>Titus Labs Document Marking for SharePoint</i> .....	12

## **Executive Summary**

SharePoint is growing quickly and is being used as a mission critical document and records management repository. Security of documents and records is critical to the ongoing viability of the organization. SharePoint's native security system has evolved from a file sharing and decentralized workgroup environment. As a result, the security is easy to set up but often does not provide the granularity and flexibility needed in mission critical environments.

In order to enhance the security of a SharePoint document repository, three key areas need to be addressed, controlling access to sensitive documents, unauthorized modification of documents, and raising the awareness of sensitive documents within the organization. In order to address these three challenges, customers should be looking for solutions that enhance security via document metadata, use PDF conversion to prevent unauthorized modification of documents, and apply document markings such as header/ footers and watermarks to enhance the awareness of sensitive information within the organization.

## **The Security Challenge in SharePoint**

The Microsoft SharePoint family of technologies forms a rapidly growing, web-based collaboration and content-management system. The Office SharePoint Server 2007 Document Management offering helps organizations realize their document management goals. A centralized repository improves information discovery and reuse of critical assets, empowering users to harness the organization's collective knowledge.

With an annual growth rate of approximately 35 percent, SharePoint is Microsoft's fastest growing server product in history. Forrester Research in 2008 indicated that 96% of enterprises are considering, planning on, in the process of, or have already completed deploying at least some part of the Microsoft SharePoint offerings, and 87% of those plan to implement or upgrade to SharePoint within the next 12 months.

As a result of its birth as a decentralized web portal, many organizations, teams and departments are independently implementing SharePoint functionality, without involvement from the central IT department. Critical documents and records are rapidly being migrated to SharePoint from more established technologies, such as file servers and legacy applications. When a new technology is adopted as quickly and organically as SharePoint has been, new risks can inadvertently be introduced.

SharePoint environments can be susceptible to the following risks:

- Users obtain access to documents that they should not have access to.
- Employees, customers, and partners download Office documents from SharePoint and then change them without authorization.
- Users share documents that are not properly labelled for security and compliance.

Let's examine these risks one at a time.

**Risk #1 - Users obtain access to documents that they should not have access to**

As the diagram shows below, there are three main elements to SharePoint security, the permissions assigned, the user or group assigned the permissions, and the object secured (site, library, document etc).

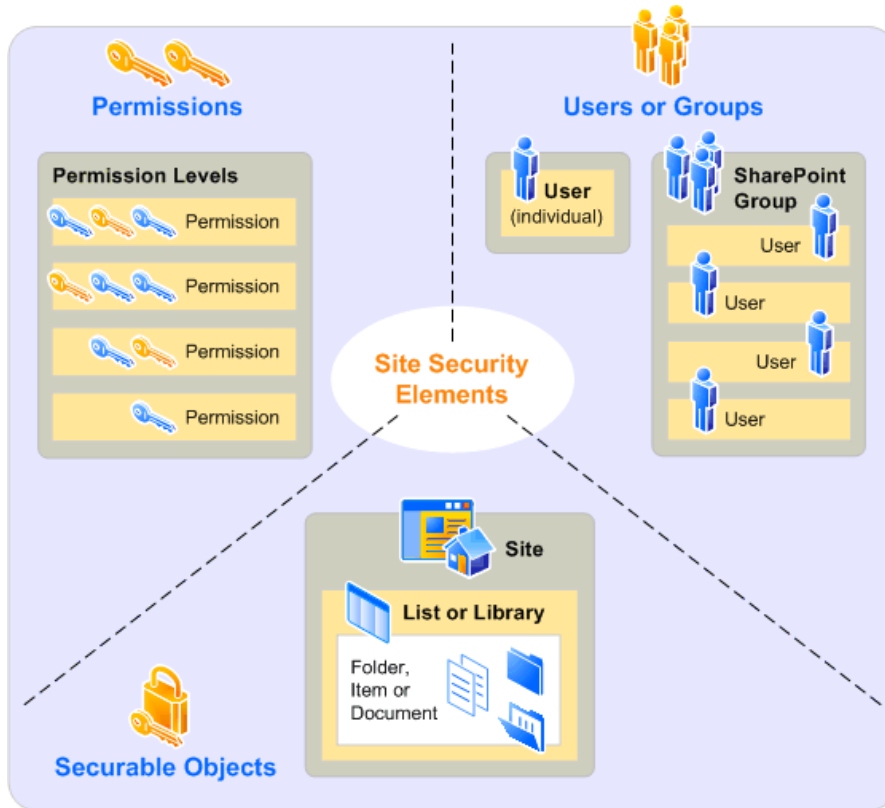


Figure 1 - SharePoint security

The standard SharePoint security model is primarily based on the concept of inheritance. Permission inheritance is the easiest way to setup security for SharePoint. By default, permissions within a sub-site or library are inherited from the site. Inheriting permissions is the easiest way to manage security for a group of sites or document libraries. However, permission inheritance assumes that

permissions for a particular document library should be the same as permissions for all the other document libraries. This is often not the case as some document libraries may contain more sensitive information.

To change permissions for a particular document library the standard inheritance model must be broken. Inheritance for any securable object at a lower level in the hierarchy can be broken by editing the permissions (creating a unique permission assignment) on that securable object. For example, you can edit the permissions for a document library, which breaks the inheritance from the site. This copies the groups, users, and permission levels from the parent site to the document library, and then breaks the inheritance. In order to setup permissions for individual documents, the administrator must define item level permissions for all the documents individually. This process can be extremely time consuming and error prone.

As a result of the difficulties associated with setting up item level permissions, many SharePoint administrators just implement the standard inheritance method of security. Unfortunately, this method does not provide the level of security needed to protect certain sensitive documents, and it may result in users getting access to documents they should not have access to.

**Risk #2 - Users download Office documents from SharePoint and then change them without authorization**

Many organizations want to share SharePoint documents internally, or with partners or customers. In some cases, they may wish to allow others to read the document, but not be able to modify the document. Most of these documents are created using Microsoft Office. Office documents can be opened in Read Only mode from SharePoint, but this does not stop someone from doing a "Save As", renaming the document and then changing it. As a result, many customers struggle with how to share documents with users that should only have read only privileges.

**Risk #3 - Users share documents that are not properly labeled for security and compliance**

Many organizations have experienced data loss when sensitive documents are sent outside of the organization. This is often due to the fact that users are not aware of the sensitivity of the document. Often, documents are created and sent around to other users with little or no control.

Many organizations have established document classification procedures, but have no way to enforce the labeling of documents. In addition, document classification procedures are seldom implemented by the users. As a result, documents are often circulated without the users' being aware of the sensitivity of the document, or of its content. This can result in inadvertent spillage of sensitive information that could expose the organization to embarrassment or lawsuits.

### **Addressing the Security Risks**

#### **Addressing Risk #1 - Controlling user access through metadata-based security**

The standard inheritance based security model works well for some situations; however it only provides a hierarchal method of security policies. This process becomes less effective when administrators want to apply different security policies to each file. In this situation, defining the security policies becomes very time consuming.

Metadata based security provides an attribute based method of security, and allows files to be granted security based on their specified metadata properties. Metadata is information you attach to your SharePoint document that provides contextual clues to its security, subject, audience, intent etc. The assigned metadata can be used to indicate the sensitivity or handling instructions for documents. For example, a metadata tag of INTERNAL USE attached to a document could indicate that the document should not be circulated outside the organization.

Within a SharePoint document library, metadata is represented as columns. By default, document libraries have columns such as Document Name, Time Modified, and Modified By. New columns can be added to SharePoint document libraries. For example, we could add a column called Classification that would be used to represent the document's classification. For this column we could allow values such as INTERNAL USE, PUBLIC, and SECRET. These values can be assigned when a user is saving a document to the document library, or can be assigned as default as documents are bulk loaded into the SharePoint document library.

A metadata based security model allows administrators to grant access to documents based on their assigned metadata properties. These rules can then be assigned to a document library. This results in specific permissions for each document in the library, without having to do tedious item-level permission assignment.

In the following example, the " Secure Library" document library contains three documents. Two of the documents have a metadata property of CONFIDENTIAL and one document has a property of UNCLASSIFIED, as shown below:

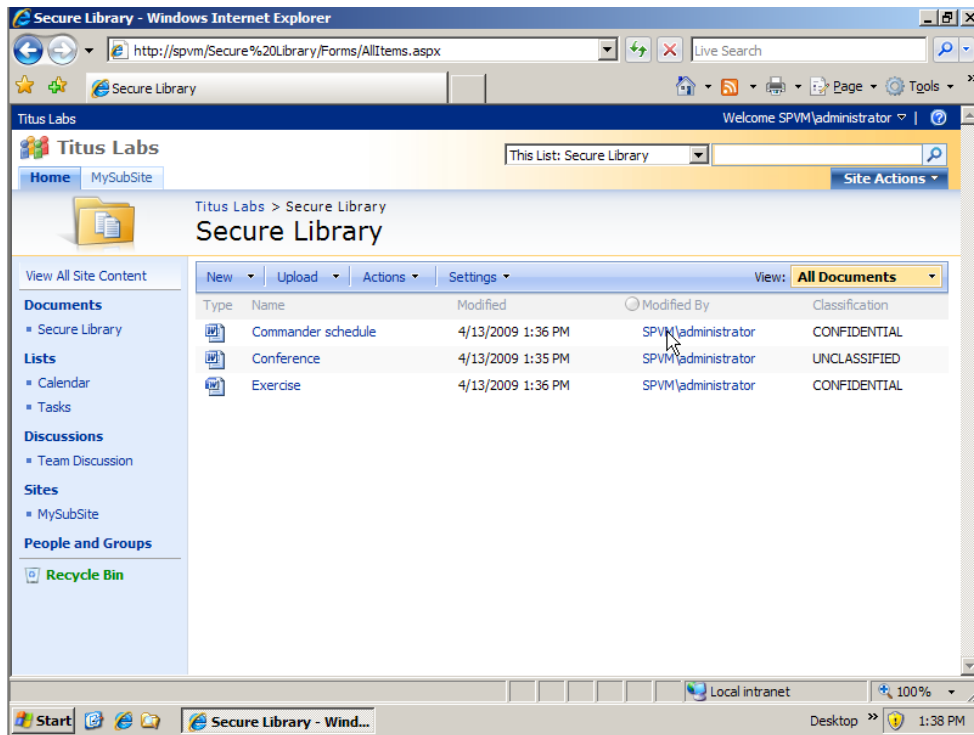


Figure 2 - Document library with metadata properties

With metadata-based security, the permissions for this document library can be configured as follows:

- All users can view UNCLASSIFIED documents
- Only Alice and Bob can view CONFIDENTIAL documents

In this scenario, Alice and Bob can view the Commander Schedule and Exercise documents, which are CONFIDENTIAL. Other users do not see these documents in the document library, since these users do not have permission to view CONFIDENTIAL documents.

**Addressing Risk #2 - Converting to PDF to prevent unauthorized document changes**

In almost all organizations there are some documents that only certain employees can change. Other employees, customers or partners should be able to view the documents, but should not be able to change them. The Microsoft Office environment provides a well known set of tools that allow employees to collaborate

and share documents. But by its nature, Office documents can be modified, copied and deleted. As a result, Office documents are not suitable for situations where organizations only want to provide a read only view of the document.

PDF – The accepted format

A PDF file is a "read only" document that cannot be altered and meets all legal requirements to be admissible in a court of law. PDF is the universally accepted format for sharing read only views of documents. PDF also serves as a "final" format for archiving and record purposes. The optimal SharePoint environment would allow employees to collaborate on building Office versions of documents, while at the same time automatically producing PDF versions of documents for sharing with users, customers or partners who should have a read only view. Having users produce PDFs is a time consuming and tedious process.

In the following example an organization has created a document library for administrative documents. Every time a new Office document is added to the document library the solution will automatically create a PDF version of the document. The solution should also allow administrators to assign permissions that restrict some users to only seeing the PDF versions.

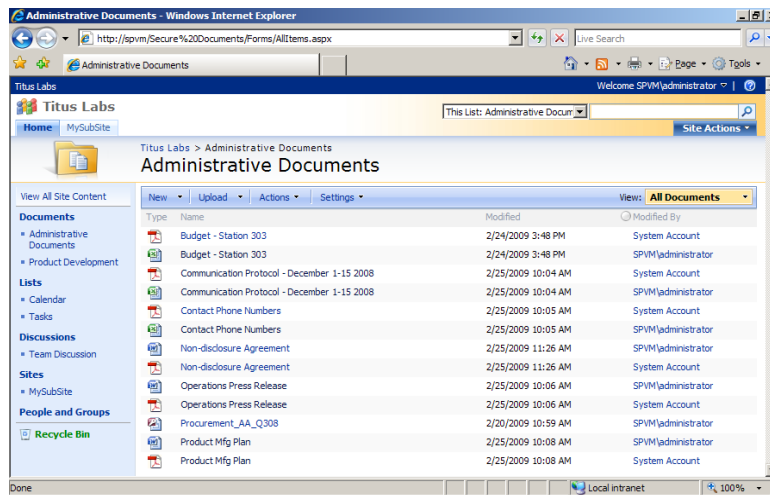


Figure 3 - PDF versions of documents are automatically created

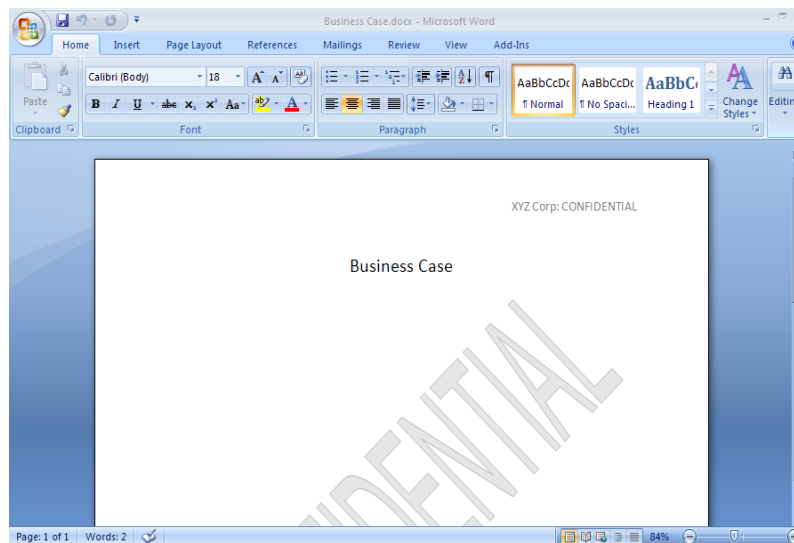
Addressing Risk #3 - Enhancing security and compliance by automatically marking documents

Many organizations have experienced data loss when sensitive documents are sent outside of the organization. This is often due to the fact that users are not aware of the sensitivity of the document. Often, documents are created and sent around to other users with little or no control.

Labeling documents with their classification can make employees aware of the sensitivity of the documents and can help ensure that users do not inadvertently forward sensitive documents outside the organization. Labels are usually placed in the header and footer of the document or in some cases as a watermark. These visual labels can indicate whether the document is INTERNAL USE, CONFIDENTIAL etc. Inserting visual labels is a simple first step in enhancing the security of sensitive organizational information.

Many organizations have established document classification procedures, but have no way to enforce the labeling of documents. As a result, document classification procedures are seldom implemented by the users. An automatic labeling solution which could take the labeling decision out of the hands of end-users, and which could ensure all documents have appropriate labels would enhance the organizations' information security.

In the following example an organization has decided to create a SharePoint document library that contains some confidential documents. When a document is added to this SharePoint document library, and the document has a metadata tag of CONFIDENTIAL, the solution should automatically add a header, footer and watermark that indicate the sensitivity of the document.



**Figure 4 - Header, footer and watermark are automatically added**

### **What to Look For in a Solution**

When looking for a solution to enhance security in SharePoint, look for the following capabilities:

- ❑ **Metadata-based security:** Look for a solution that can control access to SharePoint files based on metadata properties. This eliminates the need for administrators to define security settings for every document. The solution should support any file type and metadata property in SharePoint, including metadata security based on document attributes, content types, date, and document author.
- ❑ **Automatic PDF conversion:** Look for the ability to enable automatic conversion of Microsoft Office documents to PDF. This provides a more secure and portable document format for collaboration. The solution should support bulk conversion when a large number of documents are uploaded into SharePoint, as well as individual file conversion.
- ❑ **Document marking:** Seek a solution that automatically applies classification labels and watermarks to existing and new Microsoft Office documents. This raises user awareness and accountability, and ensures compliance with regulatory marking standards. The solution should support automatic marking for both bulk and individual files, and should enable administrators to configure and update labels at any time.
- ❑ **Integration with SharePoint:** The solution should work with standard SharePoint sites and document libraries. It should also install via a SharePoint solution package.
- ❑ **Ease of administration:** Look for a solution that is administered through standard SharePoint Information Management Policies, and leverages Microsoft Active Directory for user and group permissions.

### The Titus Labs Advantage

As the leading provider of document classification / security solutions for Microsoft Office, Titus Labs now offers a family of SharePoint security solutions. The Titus Labs family of SharePoint solutions include:

- **Titus Labs Metadata Security for SharePoint**

Titus Labs Metadata Security for SharePoint allows administrators to protect documents in SharePoint based on their metadata properties. Access to documents, and permissions associated with documents (Read, Write, Full Control etc) can be based on the document's metadata properties. This solution applies to any type of document.

- **Titus Labs PDF Control for SharePoint**

Titus Labs PDF Control for SharePoint can automatically create PDF versions of Microsoft documents as the documents are added to SharePoint. The conversion takes place transparently in the background, and requires no additional software on the user's desktop. If the source document is revised, the PDF is updated automatically, which ensures that the PDF version is always up to date.

Administrators can control the permissions on both the source document and PDF, so that some users can access the original documents, while others can see only the PDF. Both versions are stored in the same SharePoint Document Library, which makes document management easier.

- **Titus Labs Document Marking for SharePoint**

Titus Labs Document Marking for SharePoint can automatically add labels to Office documents as they are added to a SharePoint library. Labels can be added to the document header, footer, and/or watermark. The label content is completely configurable by the administrator, and can be based on text strings or derived from the document's metadata.

Titus Labs solutions are widely deployed and are in use by over 800,000 users. Customers include the United States Department of Defense, Dow Corning, US Veteran's Administration, NATO, Australian Department of Defence, and numerous other organizations.

To find out how Titus Labs can help your organization enhance SharePoint security, please visit [www.titus-labs.com](http://www.titus-labs.com).