Gimmal

Information Management for Everyone®

User Guide

Classified Records

(Feature-Activated)
For SharePoint 2013/2016

Software Version 4.13.1

January 2019

Title: *Classified Records User Guide*

© 2019 Gimmal LLC

Gimmal® is a registered trademark of Gimmal Group.
Microsoft® and SharePoint® are registered trademarks of Microsoft.

Gimmal LLC believes the information in this publication is accurate as of its publication date. The information in this publication is provided as is and is subject to change without notice. Gimmal LLC makes no representations or warranties of any kind with respect to the information contained in this publication, and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any Gimmal software described in this publication requires an applicable software license. For the most up-to-date listing of Gimmal product names and information, visit www.gimmal.com. All other trademarks used herein are the property of their respective owners.

If you have questions or comments about this publication, you can email TechnicalPublications@Gimmal.com. Be sure to identify the guide, version number, section, and page number to which you are referring. Your comments are welcomed and appreciated.

Contents

Preface

Gimmal delivers market leading content governance and compliant records solutions built on Microsoft® SharePoint®. Gimmal solutions drive user adoption and simplify information access by making information lifecycle management of content simple and transparent, ensuring consistent compliance and proactive litigation readiness enterprise-wide while lowering costs.

Gimmal's Classified Records combines with Gimmal's Compliance Suite for SharePoint to give your organization a reliable and centralized repository for collaboration and classified records management that is compliant with the standards of the Department of Defense (DoD) 5015.2 Records Management Program.

Who Should Use This Guide

This guide is intended for beginning and advanced users of the Compliance Suite software. All users must have a basic knowledge of SharePoint 2013/2016 functionality. This manual contains step-by-step instructions for using Classified Records.

Important Notes About This Manual

All illustrations are for example purposes and vary depending on how your installation is configured.

Overview

The Gimmal Classified Records application provides enhancements to Gimmal Compliance Suite that enable the management of classified records. These records are compliant with the Department of Defense (DoD) 5015.2 Standard.

The DoD supports both Classified and Standard Baseline Records. In Gimmal Compliance Suite, all records are Standard Baseline Records, while the Gimmal Classified Records product allows for the creation of Classified Records where Compliance Suite manages both record types.

Some of the Gimmal Classified Records' product features include the addition of specific security level functionality and Supplemental Markings as part of the baseline tests.

When creating a Classified Record, a mandatory security classification is required. The available security classifications are created by your records administrator and they are a special type of supplemental marking. Each security classification has a name and a rank value. Security classifications with higher rank values are automatically included into those with lower values. Users and/or groups are given access to a specific security classification. Users that are not part of a security classification applied to a classified record or that have access to a lower security classification will not be granted any access to the item. Security Classifications can be given a name and a ranking value to suit an organization's needs. For example, this guide uses "Top Secret", "Secret", "Confidential" and "Unclassified" with ranking values of 3, 2, 1, and 0.

Users that are assigned to a Security Classification of Confidential (rank =1), for example, only have access to classified records whose rank value is equal or lower (Confidential and Unclassified). When creating a classified record, the available security classifications to which the user is a member are displayed in a list when selecting the Initial Classification (an informative label) and the Current Classification (the security classification applied to the classified record). In the previous example, if John Smith, who is assigned a security classification of Confidential, will not be allowed to create or interact with any Classified Records that are higher than his level (Secret and Top Secret).

A Security Classification with a higher numeric value is automatically included into the ones with lower ranked numeric values. Users in the "Top Secret" ranking automatically have access to rankings of 2, 1, and 0. Users that are assigned to a Security Classification of Confidential (rank =1) only have access to Classified records whose rank value is equal or lower (Confidential and Unclassified).

The security classifications work in conjunction with supplemental markings and users must belong to the appropriate supplemental markings in addition to having the appropriate security ranking to access a classified record. For example, a user with Top Secret access is not given access to a classified record with supplemental markings assigned to it if this user is not part of all of the supplemental markings.

Filing Classified Records

Filing a Classified Record is the act of creating and storing records based on your organization's records management policies. Classified Records follows all of the same rules found in the "Filing Records" section of the *Compliance Suite User Guide*. In addition, retrieving, copying, moving, and editing record metadata follows the same steps as those described in the "Working with Records" section of the *Compliance Suite User Guide*.

Classified Records adds specific metadata along with extended security controls to the Compliance Suite Record content types. It also allows these elements to be added to custom content types that are derived from the parent Cs content types. An organization can leverage existing content types or build new ones based on the existing ones for greater flexibility.

Classified Records also adds conditional mandatory fields with actions that are dependent on selection choices of other fields.

Table 1 describes the metadata values that are specific to classified records along with any particular requirements.

Note
A classified record has all of the metadata of a compliance suite record content type. See the *Compliance Suite User Guide*.

Table 1 Classified Records Metadata Value

Component	Required for Population
Initial Classification	Mandatory
Current Classification	Mandatory
Reasons for Classification	Mandatory only when "Classified By" is not blank or null.
Classified By (also called classification authority)	Mandatory if "Derived From" field is blank or null.
Classifying Agency	Optional
Derived From	Mandatory if "Classified By" field is set to "none."
Declassify On	Mandatory for all but restricted data or formerly restricted data (the declassify trigger can be a date, an event, an exemption category and date, or a combination of dates and events)
Downgrade On	Optional (the downgrade trigger can be a date, an event, or a combination of dates and events).
Downgrade Instructions	Mandatory if "Downgrade On" is populated

Component	Required for Population
Reviewed On	Optional
Reviewed By	Mandatory if "Reviewed On" is populated.
Downgraded On	Optional
Downgraded By	Mandatory if "Downgraded On" is populated
Declassified On	Optional
Declassified By	Mandatory if "Declassified On" is populated.
Upgraded On	Optional
Reasons for Upgrade	Mandatory if "Upgraded On" is populated.
Upgraded By	Mandatory if "Upgraded On" is populated.

Note
Some of the available options listed in Table 1 might not be present because of smart filtering, which hides certain elements or makes them unavailable if they are not in the correct context. For example, you cannot upgrade a record if you are at the highest rank value or downgrade a record that is at second lowest rank value (as this is considered a declassification), therefore, these options are unavailable.

Creating a Classified Record

To create a classified record, follow these steps:

1   Navigate or search for the library where you want to add the record.

2   Click **Add new item**. The Submit Document window displays.
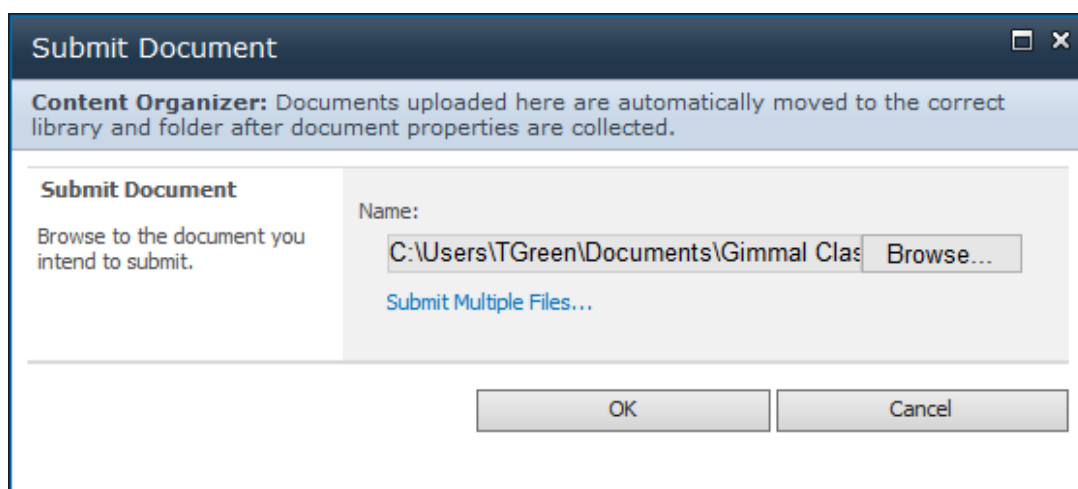
Figure 1 Submitting a Document

---

3   Browse to the location of the document and select it.

4   Click **OK**. The Drop Off Library filing form displays.

Figure 2 Drop Off Library

5   Enter the required fields for the record.

6   Select the checkbox next to **Classified Record**. The page expands to display the fields required for a classified record.

Figure 3 Fields Required for a Classified Record

7   Enter the required fields for a classified record.

8   Click **Submit**. The document is saved to the specified library and folder.

Reviewing Classified Records

Classified records can be reviewed periodically by any member of the RMA Security Officer group and their review status can be updated on the record form itself.

To review a classified record, follow these steps:

1   Navigate to a Classified Record or perform a search and choose **Edit** from the pull-down menu.

2   Enter a date in the **Reviewed On** field. Once the date is entered the Reviewed By field becomes mandatory.

3   Enter the user or organization that has performed the review.

Figure 4 Reviewing a Classified Record

4   Click **Save** to commit the changes.

Note
Records can be reviewed again by performing the same steps and replacing the values.

Grading Classified Records

Classified Records can be upgraded, downgraded, or declassified by any member of the RMA Security Officer group. The officer can manually change the current value of Current Classification in the record properties or schedule a downgrade or declassification to occur at a future date. Classified Records are graded through the record properties.

Figure 5 Sample Record Properties

Upgrades must be performed manually and immediately. A Gimmal Downgrade Timer job is responsible for performing the automated downgrades and declassification operations.

Upgrading Classified Records

A security officer can upgrade a classified record's security classification by changing its **Current Classification** value in the record properties to a higher rank. The rank values display in descending order. Selecting a value with a higher rank in the list sets the Classified Record's security to adhere to the new value.

Note
Upgrades cannot be scheduled and are performed immediately.

1. Log in as any user that is a member of the RMA Security Officers Group and navigate to the record you want to upgrade.

Note

See your RMA Administrator if you are not assigned to the RMA Security Officers Group.

---

2. Click the down arrow next to the Classified Record and select **Edit Properties**. The Record and its properties display (see Figure 5).

3. Scroll down to **Current Classification** and select the higher ranking. In the following example, the Classified Record currently graded as Secret is upgraded to Top Secret.
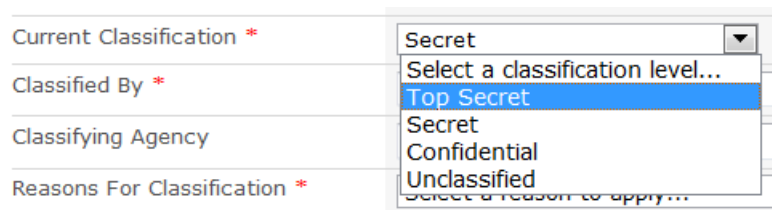

Figure 6 Upgrading a Classified Record

4. Enter the **Reasons for Upgrade** in the field that displays when you upgrade a record.

5. **Upgraded By** also displays and populates with the user's login ID. You can change the ID, if desired.

6. Save the record.

Note

Any users that are not assigned access to the new value do not see the record or have the ability to search for it.

Downgrading Classified Records

A security officer can manually and immediately downgrade a classified record's security classification by changing its **Current Classification** value to a lower rank (but not the lowest rank as this is considered declassifying a record). The rank values display in descending order. Selecting a value with a lower rank in the list sets the Classified Record's security to adhere to the new value once it is saved. A security officer can also schedule a downgrade to occur after a certain period of

time, when a specific event occurs, or when a date and an event occur (the latest value in this case is taken as the date to downgrade).

Manually Downgrading a Classified Record

1   Log in as any user in that is a member of the RMA Security Officers Group and navigate to the record you want to downgrade.

Note
See your RMA Administrator if you are not assigned to the RMA Security Officers Group.

2   Click the down arrow next to the Classified Record and select **Edit Properties**. The Record and its properties display.

3   Scroll down to **Current Classification** and select the lower ranking. In the following example, the Classified Record with Top Secret is downgraded to Secret.

Initial Classification *	Top Secret
Current Classification *	Secret
Classified By *	John Smith

Figure 7 Downgrading a Classified Record

Note
The lowest level listed in the Current Classification (the one that is assigned a rank of 0) is not available as a value to downgrade to as that is a declassification, which is explained further in "Declassifying Classified Records."

4   Save the record.

Scheduling a Downgrade of a Classified Record

1   Log in as a Security Officer and navigate to or search for the record you want to downgrade.

2   Click the down arrow next to the Classified Record and select **Edit Properties**. The Record and its properties display (see Figure 5).

3   On the record form, locate the **Downgrade On** section and select **Date**, **Event**, or **Date and Event** and enter the corresponding mandatory fields.

4   If you select **Date**, the form refreshes to show three additional fields that are mandatory:

Figure 8 Downgrade On Date Selections

5   If you select **Event,** a drop-down list of configured events displays. Once you select the event, this is the date on which the record is declassified. See the *Compliance Suite User Guide* to review how events are created and set.

6   If you select **Date and Event**, both values must be present before a record is declassified and the latest date between date and event is the date on which downgrade occurs.

7   Select a **Target Downgrade Classification**. Only classifications that are lower in rank than the current active classification display.

Note
You cannot select the lowest classification because that would be Declassification.

Figure 9 Target Downgrade Classification Selection

8   Save the record. A Gimmal Downgrade Timer job automatically downgrades the record to the target downgrade classification when it is run.

Declassifying Classified Records

Classified records become declassified after a certain period of time, unless they are deemed to contain sensitive information.

A security officer can declassify a classified record manually or it can be scheduled to be automatically declassified. A Records Manager subsequently reviews the exported declassified record and purges the latter from the system using the declassification report.

When adding a Classified Record into the record's system, **Declassify On** is set to a defaulted value that auto-calculates the date for declassification. This date is determined by taking the record's value for the **Publication Date** and adding the default classification timeframe in years as set by the records manager. A classified record can alternatively be declassified by a selected date or event or a date and an event. In the case of a date and an event, the latest date is always used for any calculation.

Manually Declassifying a Classified Record

1   Log in as a Security Officer and navigate or search to the record to declassify.

2   Click on the pull-down next to the record and choose **Edit Properties** from the context menu.

3   Set the **Current Classification** value to the value with the lowest ranking. The rank value of the lowest classification security level must be set to 1 (see *Classified Records Administration Guide*). In Figure 10, the Classified Record with Top Secret is downgraded to Unclassified.

Figure 10 Declassifying a Record

4   The conditional mandatory field called "Declassified By" displays and contains the current username performing the action. It can be changed, if desired.

5   Save the record. The record's metadata and its binary content automatically saves to a location specified by the administrator for review. The record remains in the system until the records manager performs the Declassification review from the Declassification report and purges the latter from the system completing the process.

Rescheduling Declassification of a Classified Record

1   Log in as a Security Officer and navigate or search to the record for which to reschedule declassification.

2   Click the pull-down next to the record and choose **Edit Properties** from the context menu.

3   In the **Declassify On** section of the record's form, change the current selection if a specific date and/or event is required by selecting the appropriate radio button and entering the information.

4   Save the record. A Gimmal Declassification Timer job automatically declassifies the record when the date is reached.

Working Papers

Working papers provide a separate non-record area for work in progress on classified information. These are not records, but they contain classified security information. They can optionally be converted into a classified record. They can be considered a precursor to a document that someone is offering that contains classified information. Working papers are retained for a set period of time.

Working papers contain some specific metadata. Documents do not have to be a working paper in order to become a classified record.

Working papers have supplemental markings, which are document markings not necessarily related to classification markings. These markings elaborate on or clarify document handling.

When working records are declared as classified records, the previous values for supplemental markings and security level are stripped.

This chapter contains procedures for the following:

- Creating, editing, and deleting working papers
- Filing working papers as formal records
- Running a working paper report

Creating, Editing, and Deleting Working Papers

With edit rights, you can add a working paper to a library that contains working papers as a content type. The security controls are the same as classified records; an end-user only sees classification levels equal or lower to which they have been assigned and those supplemental markings of which they are a member.

Creating a Working Paper

1   Click the **Add new item** link. The Upload Document window displays.

2   Browse to the document you want to upload and click **OK**.

3   Change the **Content Type** to **Working Paper** after document has been uploaded or saved. The metadata specific to a working paper displays. Alternatively, you can take an existing document and change its metadata to that of a working paper.

4   Enter the mandatory metadata elements and select an **Initial** and **Current Classification**. Not all entries may display as the list is filtered by the Classification level to which you are assigned (values equal to and lower display).

Figure 11 Working Paper Metadata Elements

5   Select any supplemental markings that you wish to place on the working paper to further limit access. Only those markings to which you are assigned display.
Click **Save**.

Editing a Working Paper

1   Select the working paper from the library. The Working Papers page displays.

2   Click the down arrow next to the working paper you want to edit and select **Edit Properties**. The document properties display.

Figure 12 Working Paper Properties

3   Edit the information you want to change and click **Save**.

Deleting a Working Paper

1   Select the working paper from the library. The Working Papers page displays.

2   Click the down arrow next to the working paper you want to delete and select **Delete**.

3   When the dialog box asking if you are sure you want to delete the working paper displays, click **OK**.

Filing Working Papers as Formal Records

After you have added a working paper to your library, you can file it as a formal record.

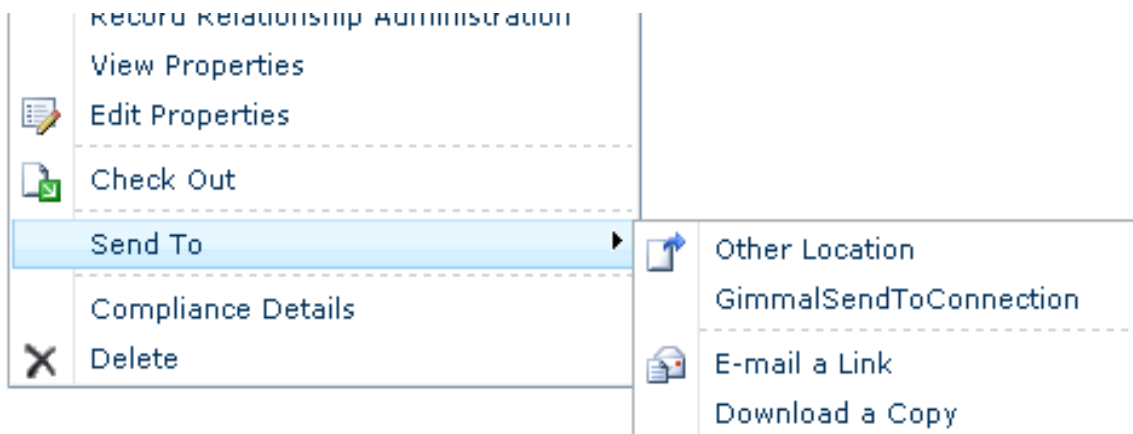1   Browse to your working paper, and from the context menu select **GimmalSendToConnection**.

Figure 13 Selecting GimmalSendToConnection

2   Click **OK** to confirm the move. The Working Paper moves to the Drop Off Library.

3   If you have RMA permissions, browse to the Drop Off Library and locate the document.

4   Click the down arrow next to the document and select **Edit Properties** from the drop-down menu. The properties window displays.

5   Change the content type to the appropriate content type (e.g. RMA Record), and enter the required classified record properties, including Filing Location.

6   Click **Save**.

Running a Working Paper Report

A working paper report shows what documents are designated as working papers in the system. Any member of the RMA Security Officers group can run this report.

Follow these steps to run a working paper report:

1   To access the Work Paper Report page, select **Site Actions** -> **Site Settings** -> **Classified Records** -> **Working Paper Reporting**.

Figure 14 Working Paper Report Selection

The Working Paper Report page displays.

Figure 15 Working Paper Report Page

2   Enter a unique title for the report in *Working Paper Report Title*.

3   In **Current Classification**, select the classification level you want to include in this report.

4   Enter any user IDs who may have created the report in **Created By**.

5   In **Created Date**, enter the date range to search.

6   Specify the destruction date for working papers in **Destruction Date.**

7   Select the sites to search and click **Submit**.

Glossary

The following terms are used in this guide:

- Classified Records – Contain information that is not public. These records become public after a specified period of time. There can be separate repositories for classified and public records. Once records are declassified, they are expunged and transferred to a public accessible repository.
- Security Classifications – Special types of Supplemental markings placed on a Classified Record. Available values are selected from a security trimmed list called initial classification and current classification on the classified record form. The initial classification value serves as a marker while the current classification locks down the classified record to only those user's that have equal or higher access (called a rank value) for the entry selected.
- Conditional Mandatory Elements – Certain attributes when entered on the records form will cause other metadata elements to become mandatory as a result.
- Classification Guides – The guides provide a template that automatically populates certain metadata attributes on the classified records form when selected.
- Working Papers – Documents that contain classified information that must be protected and, as a result, have Security Classifications and optional Supplemental markings applied to them. They also have a finite existence if they are not declared as classified records as they are purged from the system after a set period of time that is by default 180 days but configurable by an administrator.