

Security and Access Controls

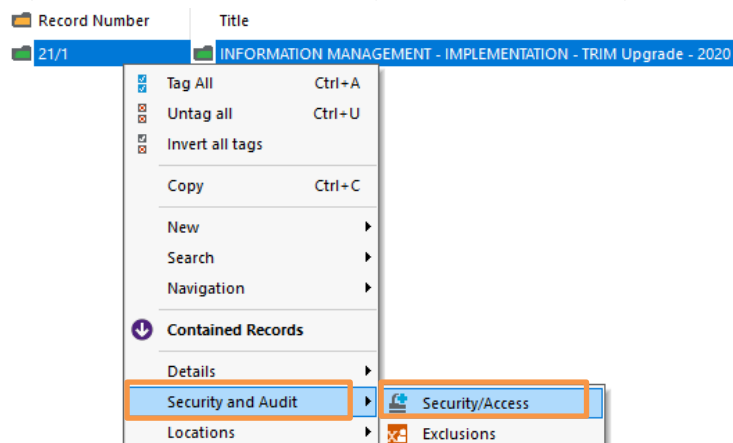
Security Levels, Active Security Caveats and Access Controls are used to control access to records in TRIM9. These are generally set at the folder (file) level and are applied at the time that the folder (file) is created. Sometimes they will be set automatically (e.g. some Classifications will automatically copy over certain security settings), otherwise they must be set manually when the folder (file) is created.

By default, records (documents, emails, sub-folders etc.) placed within a folder (file) will inherit the Security Level, Active Security Caveats and Access Controls from the folder (file) they are placed within.

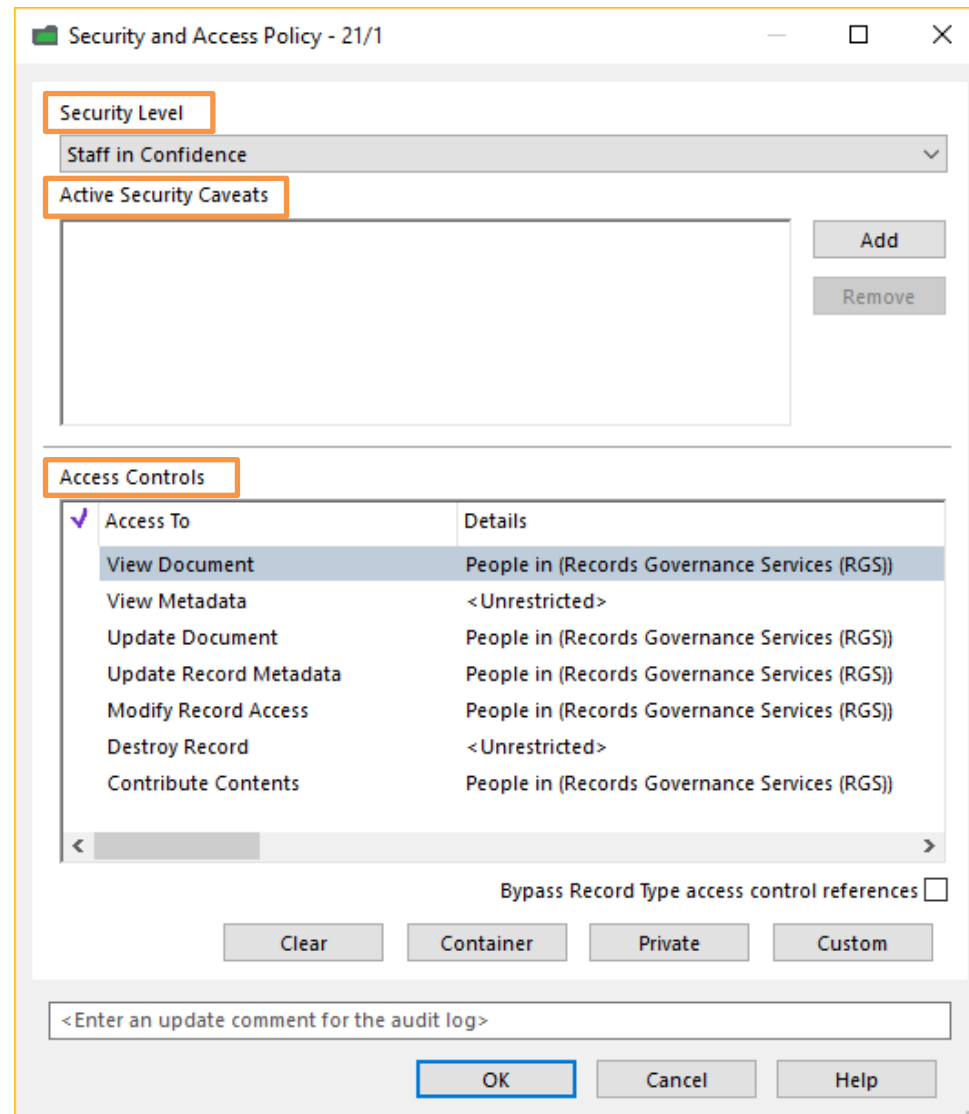
For this reason, where appropriate it is recommended that Security and Access Controls are managed at the folder (file) level, as it is generally easier and cleaner to maintain these settings at the folder (file) level so that all the records placed within that folder (file) inherit the required security settings. However, individual documents/emails or sub-folders can have their Security and Access Controls set differently to the settings on the folder (file) when this is appropriate to do so. On this note, if a document/email or sub-folder is moved to another folder (file) it will retain its Security Level and Active Security Caveats, however by default it will inherit the Access Controls from the new folder (file).

Although Security and Access Control settings are set at the time a folder (file) is created, they can be updated at any time. Below are instructions on how to do this:

1. Locate the record (generally a folder (file) but can be any record type if appropriate).
2. Right-click on it and select **Security and Audit** → **Security/Access**



3. The 'Security and Access Policy' window will display. Note the **Security Levels**, **Active Security Caveats** and **Access Controls** sections of this window:



Security Level

Security Levels in TRIM9 ensure that records can only be accessed by users who have the same or higher Security Level (on their TRIM9 Profile) than that allocated to a record. The Security Level on a user's TRIM9 Profile is dependent upon their role within the organisation; and set and managed by Records Governance Services.

The default 'Security Level' is **Staff in Confidence**. However, some Classifications placed on a folder (file) will automatically populate this field with a higher Security Level. Generally, whatever is prepopulated in the 'Security Level' field should be sufficient, as Access Controls (discussed below) are primarily used at UON to control access to records in TRIM9. However, if you are dealing with sensitive information which should have a higher Security Level on it, you can customise the Security Level of a record as per the below instructions:

- Click the **drop-down** button at the end of the 'Security Level' field:

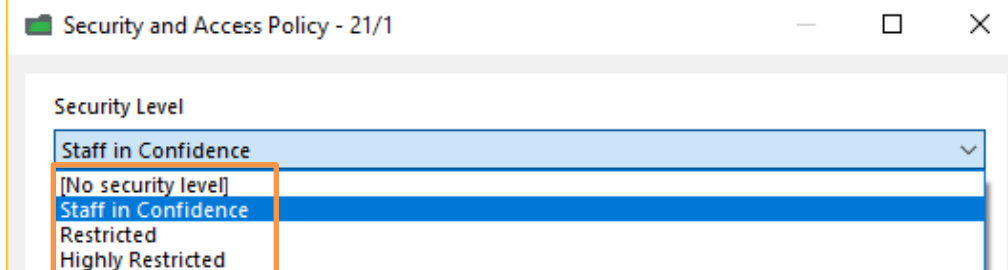


Security and Access Policy - 21/1

Security Level

Staff in Confidence

- Select the most suitable Security Level for your record from the options which display:



Security and Access Policy - 21/1

Security Level

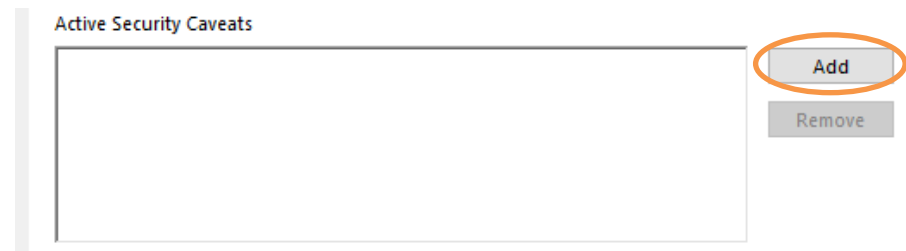
- Staff in Confidence
- [No security level]
- Staff in Confidence
- Restricted
- Highly Restricted

Active Security Caveats

Active Security Caveats in TRIM9 ensure that records with a particular Security Caveat on them can only be accessed by users who have the same Security Caveat (on their TRIM9 Profile). The Active Security Caveats on a user's TRIM9 Profile are dependent upon their role within the organisation; and set and managed by Records Governance Services.

By default, the majority of TRIM9 records will not have an Active Security Caveat assigned to them. However, some Classifications placed on a folder (file) will automatically apply an Active Security Caveat to the folder (file). Generally, whatever is prepopulated in the 'Active Security Caveats' field should be sufficient, as Access Controls (discussed below) are primarily used at UON to control access to records in TRIM9. However, if you are dealing with information which requires a Security Caveat to be applied to it, you can add one or more Security Caveats to a record as per the below instructions:

- Click the **Add** button to the right of the 'Active Security Caveats' field:

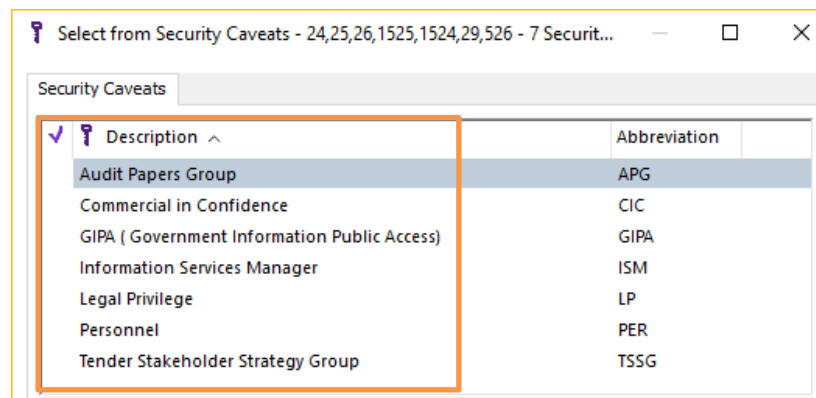


Active Security Caveats

Add

Remove

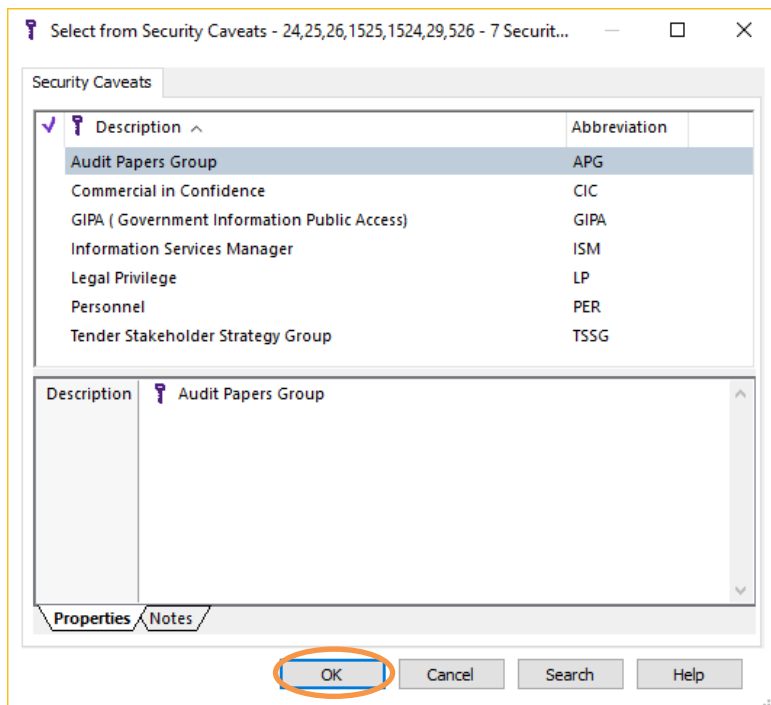
- The **'Select from Security Caveats'** window will appear. Select any applicable Security Caveats (or select multiple by clicking to the left of them to tag them):



Select from Security Caveats - 24,25,26,1525,1524,29,526 - 7 Securit...

Security Caveats	Description	Abbreviation
<input checked="" type="checkbox"/>	Audit Papers Group	APG
<input type="checkbox"/>	Commercial in Confidence	CIC
<input type="checkbox"/>	GIPA (Government Information Public Access)	GIPA
<input type="checkbox"/>	Information Services Manager	ISM
<input type="checkbox"/>	Legal Privilege	LP
<input type="checkbox"/>	Personnel	PER
<input type="checkbox"/>	Tender Stakeholder Strategy Group	TSSG

8. Click **OK** to close the 'Select from Security Caveats' window:



Note: Security Levels, Active Security Caveats and Access Controls (explained below) all work in conjunction, not separately. I.e. Even if a user is listed in the Access Controls for a record, if that record also has an Active Security Caveat added to it, the user would need that Active Security Caveat to be present on their TRIM Profile (TRIM Profiles are managed by Records Governance Services) in order for them to be able to access that record. This is important to consider when increasing the Security Level or adding an Active Security Caveat to a record.

Access Controls

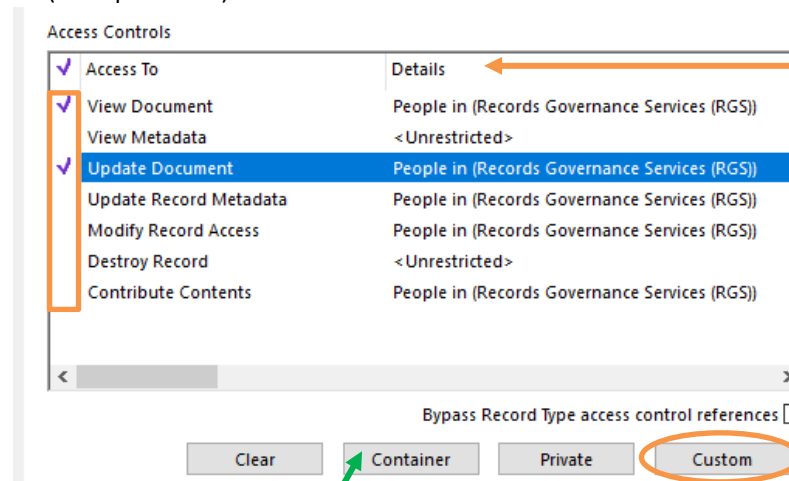
Access Controls are Security controls which can be applied to control access to records within TRIM9. Access can be granted to users or groups of users. This is particularly useful when the contents of a folder are confidential and only a selected group of users should have permission to view the records.

At UON, Access Controls are the primary way of controlling access to records in TRIM9. Below is listed the seven available Access Controls, and an explanation of the purpose of each one:

Access Control	Purpose
<i>View Document</i>	Permits those listed to view the folder and documents within it – users must also have the “View Metadata” permission to view the document.
<i>View Metadata</i>	Permits those listed to view the title and metadata of the folder and its contents, but NOT actually open the document and view it. Users must have the “View Document” permission to view any documents inside the folder.
<i>Update Document</i>	Permits users listed to edit documents within the folder.
<i>Update Record Metadata</i>	Permits users listed to make changes to the record metadata. E.g., Update the title.
<i>Modify Record Access</i>	Permits users listed to make changes to the Security and Access Controls on a record.
<i>Destroy Record</i>	Users are unable to destroy records so this can remain as <Unrestricted> .
<i>Contribute Contents</i>	Permits users listed to save documents inside the folder.

To make changes to the 'Access Control' field:

9. First, take note of any Locations currently listed on the Access Controls (if any) in the 'Details' column. Then, place a tick next to any Access Controls you wish to change (example below) then click **Custom**:

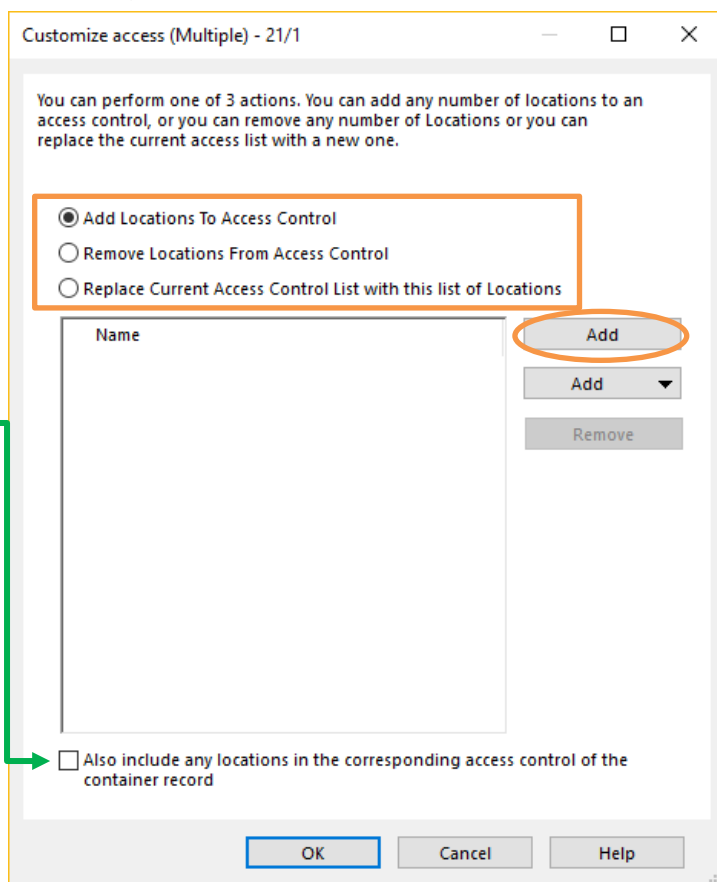


Hint: If the record you are updating is in a Container, the 'Container' button can be used to inherit the selected Access Controls from the Container.

10. The 'Customize access' window will appear. As the below window explains, you can perform one of three actions:

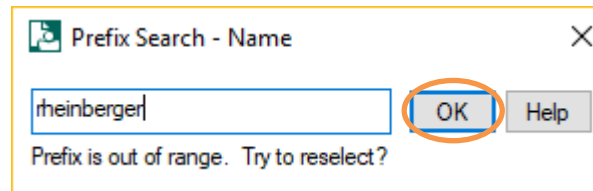
- The first option will keep any Locations currently on your selected Access Control(s) (if any) and add in any number of new Locations.
- The second option will remove any number of Locations from your selected Access Control(s) (if any).
- The third option will replace the Locations currently listed on your selected Access Control(s) (if any) with a new list of Locations.

Select the option you want to perform, then click **Add**:

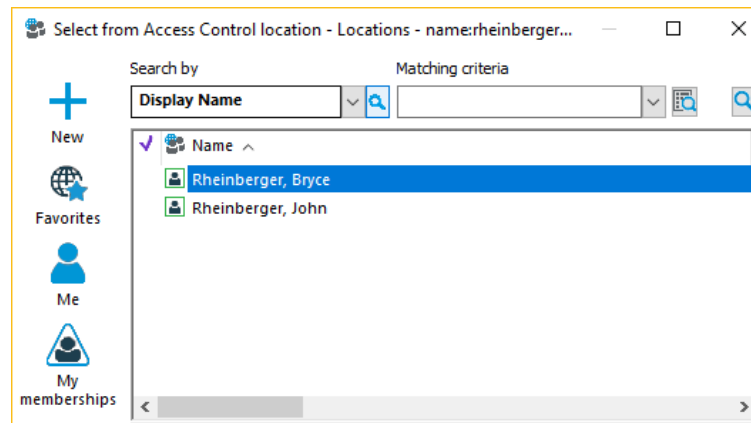


Hint: If the record you are updating is in a container, placing a tick in this checkbox will copy over any Locations in the container's corresponding Access Control(s) (the Access Controls which you selected at Step 9 above).




11. The 'Select from Access Control location' window will appear. **Don't click anywhere**, but instead just start typing the surname of the person or the name of the Position, Unit/Team you wish to add. When you start typing the 'Prefix Search – Name' window will pop up. Click **OK** to run the search:




12. The list of matching Locations will appear:



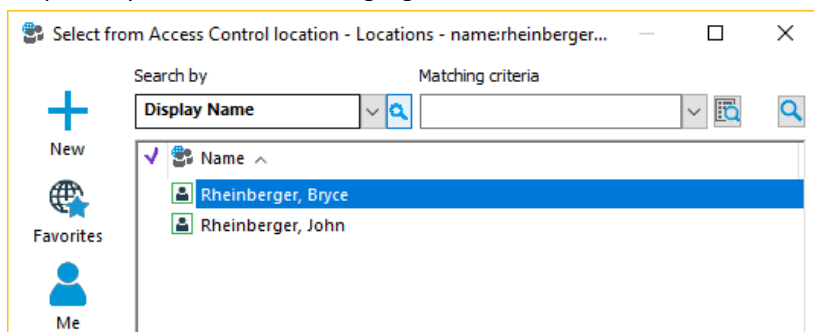
Hint: When selecting Locations to grant access to, select:

- A Green **Organisation** Location  and/or
- A Green **Group** Location  and/or
- A Green **Position** Location 

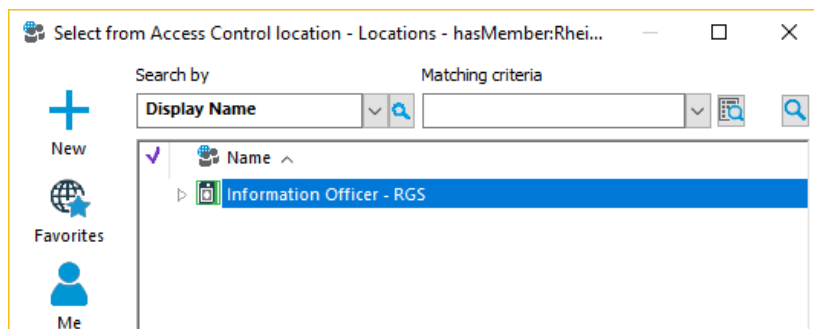
Do Not select a Person Location  because if that person transfers to a different Team, Unit, School, Faculty etc. it will likely be no longer appropriate for them to have access to that folder.

Hint: An easy way to locate a 'Position' Location such as 'TRIM Administrator' or 'Manager Records Governance Services', or other Location such as a School or Business Unit is;

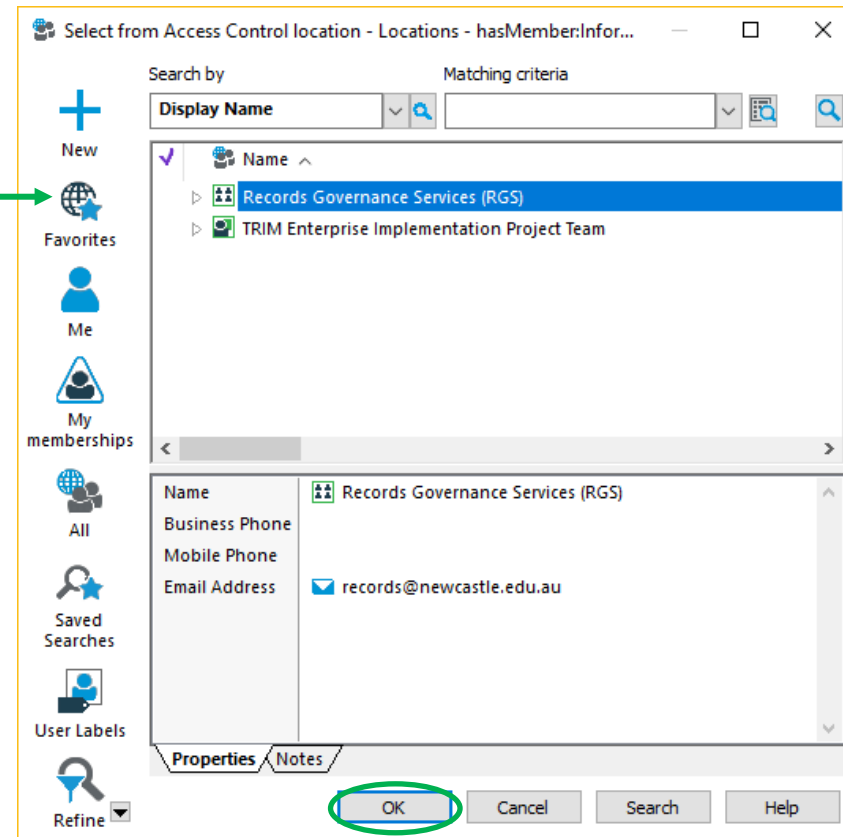
- At Step 11 (refer previous page) search for a person who is in that Location.
- Then, when the **'Select from Access Control location'** window appears click on the person you searched for to highlight them blue:



- Then, press **Ctrl+J** on the keyboard to navigate one level up the TRIM9 Locations Hierarchy.
- Examples:
- o If you press **Ctrl+J** on a **Person** Location, TRIM9 will likely display that person's **Position** Location, or **Team/Business Unit** Location they are a member of.
 - o If you press **Ctrl+J** on a **Business Unit** or **School** Location, TRIM9 will likely display the **Division** Location or **College** Location which that Business Unit or School resides under.



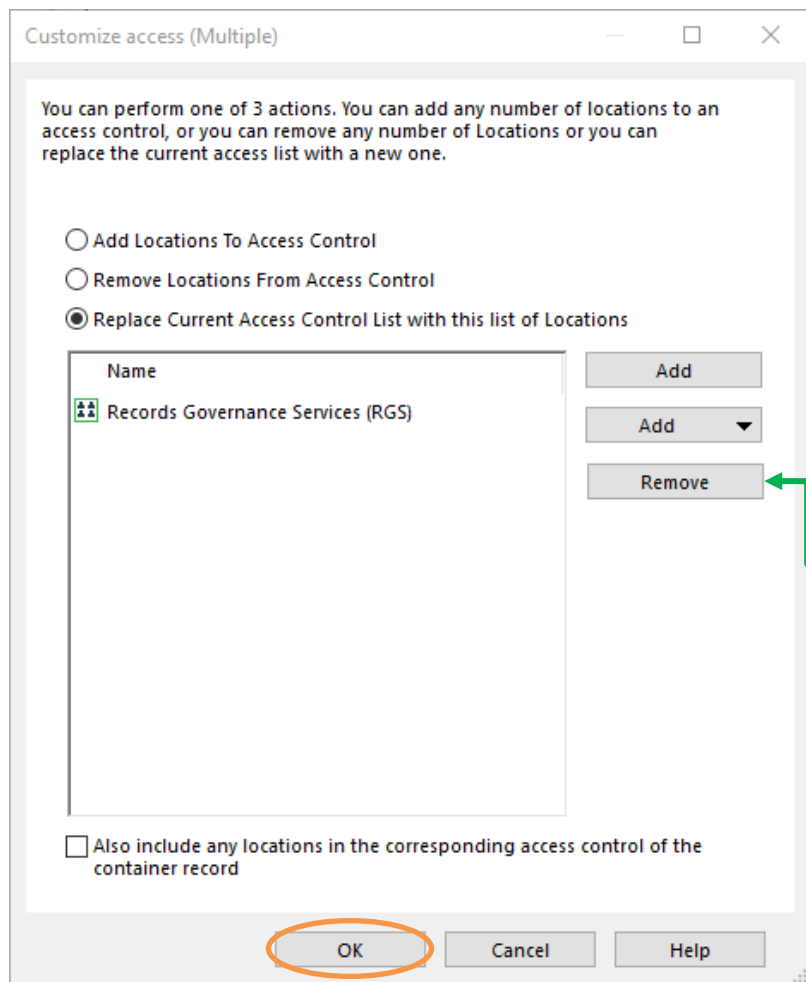
- If necessary, you can continue to use **Ctrl+J** to navigate up the TRIM9 Locations Hierarchy until you have located the Position/Business Unit/School etc. Location you want to select. Once you have located the Location you want to select, click on it once to highlight it blue, then click **OK**:



Hint: If there are TRIM9 Locations which you think you will need to use regularly; you can add them to your Favourites by right-clicking on them → **Send To → Favorites**

Then in future when you're looking for a Location in a Locations window such as the one above, you may be able to click on the **Favorites** button to easily find it.

13. The Location(s) you added will now be displayed in the **'Customize access'** window. If necessary, you can repeat the above steps to add additional Locations. When you're ready, click **OK** to close the **'Customize access'** window:




You can perform one of 3 actions. You can add any number of locations to an access control, or you can remove any number of Locations or you can replace the current access list with a new one.

☐ Add Locations To Access Control

☐ Remove Locations From Access Control

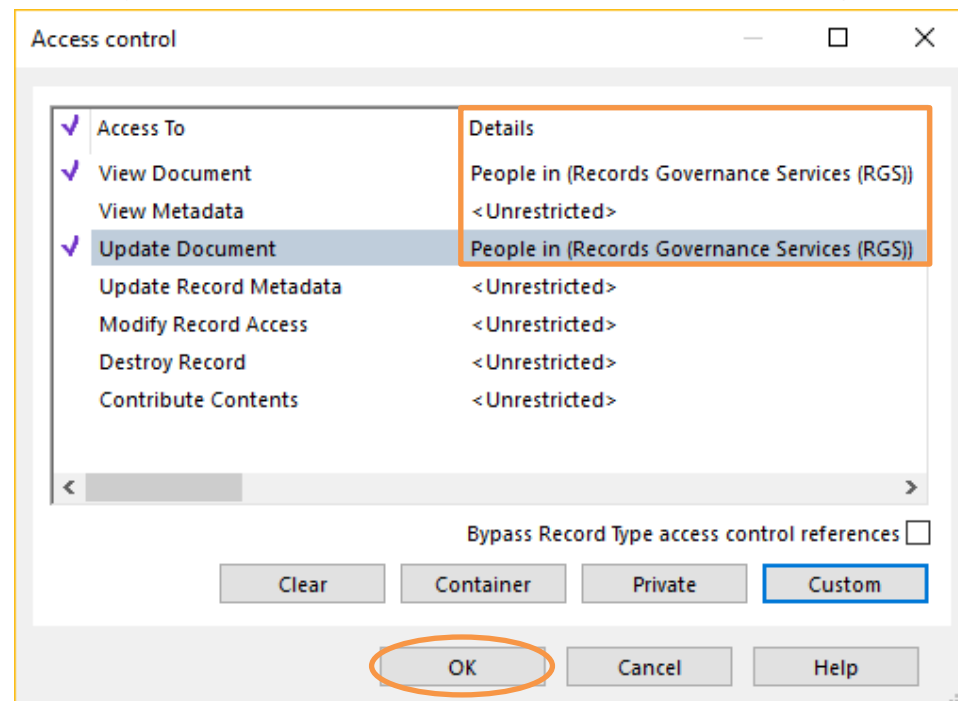
☒ Replace Current Access Control List with this list of Locations

Name
 Records Governance Services (RGS)

☐ Also include any locations in the corresponding access control of the container record

Hint: If you have added a Location but now want to remove it, if you click on it once to highlight it blue you can then use the **Remove** button to remove it.

14. You can see the changes to the Access Controls under the 'Details' column. If necessary, you can repeat the above steps to make further changes. When you're ready, click **OK** to close the **'Access control'** window and save the changes:



Access To	Details
<input checked="" type="checkbox"/> Access To	People in (Records Governance Services (RGS))
<input checked="" type="checkbox"/> View Document	<Unrestricted>
<input type="checkbox"/> View Metadata	<Unrestricted>
<input checked="" type="checkbox"/> Update Document	People in (Records Governance Services (RGS))
<input type="checkbox"/> Update Record Metadata	<Unrestricted>
<input type="checkbox"/> Modify Record Access	<Unrestricted>
<input type="checkbox"/> Destroy Record	<Unrestricted>
<input type="checkbox"/> Contribute Contents	<Unrestricted>

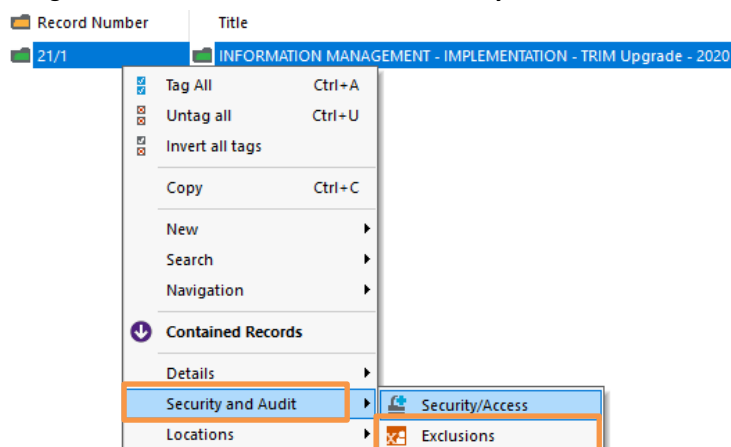
Bypass Record Type access control references ☐

Access Controls – Exclusions

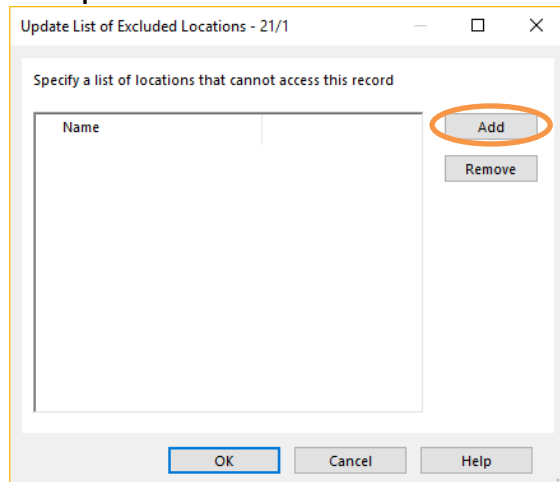
It is also possible to exclude Locations from accessing records. I.e., Even if a Location meets the security settings (Security Level, Active Security Caveats and Access Controls) of a record, if they are listed as an Excluded Location on that record then they still won't be able to access that particular record.

To add or remove an Excluded Location on a record:

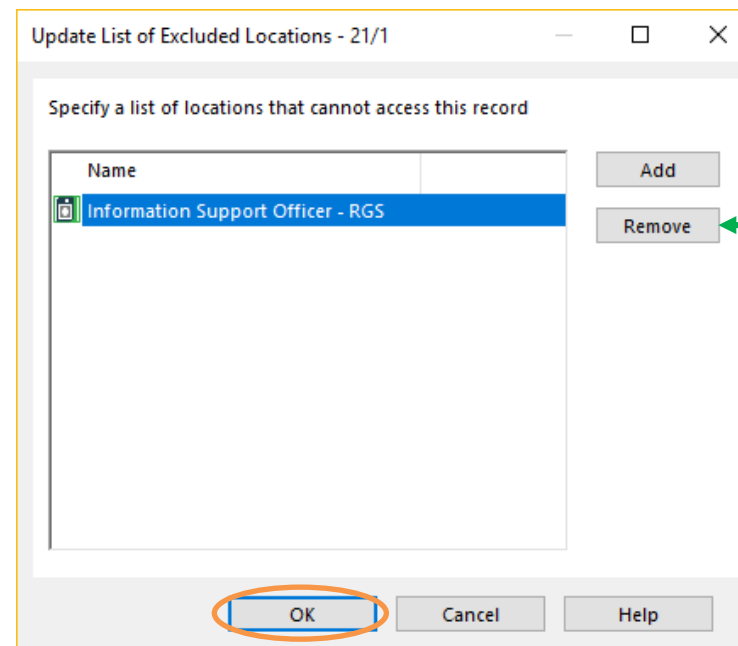
1. Right-click on the record and select **Security and Audit → Exclusions**:



2. The **'Update List of Excluded Locations'** window will appear. Click the **Add** button:



3. The **'Select from Access Control location'** window will appear. Search for and select the Location(s) which you want to add as an Excluded Location. Refer to [Steps 11 and 12](#) above if you require assistance with this.
4. The Location(s) you added will now be displayed in the **'Update List of Excluded Locations'** window. If necessary, you can add additional Locations by clicking the **Add** button again. When you're ready, click **OK** to save your changes and close this window:



Hint: If you have added a Location but now want to remove it, if you click on it once to highlight it blue you can then use the **Remove** button to remove it.