

VITA Portfolios Security Overview

I. VITA Portfolios Security Policy is Inclusive

This means that the VITA Portfolios system includes everyone by default - all VITA Portfolios users can read any production configuration and data without being a member of at least one named user group.

II. Administrator Policy

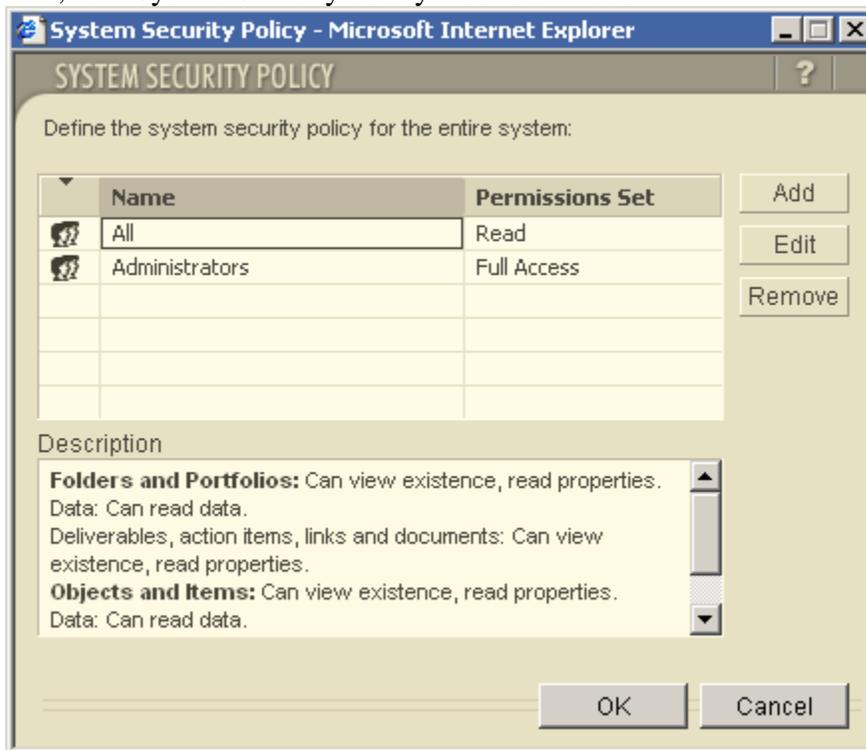
The current policy for administrators at VITA is to allow all administrators full access to all objects, folders, items and portfolios in the system.

III. The System Security Policy

The highest level of security is the "System Security Policy". Whatever is defined in this policy will automatically be "inherited" by all objects, folders, item and portfolios.

The goal in setting the "System Security Policy" is to define the broadest security permission sets to the most common set of user groups and roles.

At VITA, the "System Security Policy" looks like this:



A. The "All" User Group

This user group contains all users who have a ProSight Portfolios Login ID. They have "Read" permissions to all objects and data unless specifically noted. The "Read" permission set has the following permissions:

Folders and Portfolios: Can view existence and read properties.

Data: Can read data.

Deliverables, action items, links and documents: Can view existence and read properties.

VITA Portfolios Security Overview

Objects and Items: Can view existence and read properties.

Data: Can read data.

Deliverables, action items, links and documents: Can view existence and read properties.

B. The "Administrators" User Group

This user group contains all the users who need to be able to view or modify anything in the Portfolios system. The System Security permission set for Administrators is "Full Access".

The "Full Access" permission set has the following permissions:

Folders and Portfolios: Can view existence, read properties, create objects inside this folder, edit properties, remove objects, and change security.

Data: Can read data, update data and cell properties, and change data security in cell properties.

Deliverables, action items, links and documents: Can view existence, read properties, create, edit properties, remove, and change security.

Objects and Items: Can view existence, read properties, edit properties, remove objects, and change security.

Data: Can read data, update data and cell properties, and change data security in cell properties.

Deliverables, action items, links and documents: Can view existence, read properties, create, edit properties, remove objects, and change security.

IV. Additional Roles and User Groups

The following additional user groups are used at VITA:

A. The "Manager" Role

The "Manager" role is a system defined role. It is not a user group, but has a permission set assigned in the same way as a user group. Whoever is the Manager of an item or a portfolio will be included in the permission set of the Manager role. The Manager is a system category defined in the Setup wizard for items and portfolios. It is also displayed on some forms (e.g. it is currently labeled "Prepared By:" on the first tab of the Project Business Alignment form). By default, the system assigns the user who creates the item or portfolio as the Manager. You must have Admin privileges to change the user named in the Manager for an item or portfolio. Within the Commonwealth, Managers do not have Administrator privileges.

The permission set for the Manager role is "Custom" for predefined agency portfolios. That means that managers can do the following for any of their items that have an agency Home Portfolio:

Portfolios: Can view existence, read properties and create items inside this portfolio.

Data: Can read portfolio (summary) data.

Deliverables, action items, links and documents: Can view existence and read properties.

Items: Can view existence, read properties and edit properties.

VITA Portfolios Security Overview

Data: Can read data, update data and cell properties.

Deliverables, action items, links and documents: Can view existence, read properties, create, edit properties, and remove objects.

Note: Other pre-defined portfolios have different security settings. These are detailed in subsequent sections.

B. The "Owner" Role

The "Owner" role is similar to the Manager role, but it only applies to owners of objects (such as Scorecards) and folders. Whoever is defined as the Owner of an object or folder will be included in the permission set of the Owner role. The Owner is defined in the Setup wizard for folders and objects (categories, scorecards, forms, etc.). By default, the system assigns the user who creates the object or folder as the Owner. You must have Admin privileges to change the Owner of folder or object. At VITA, Owners do not have Admin privileges.

In general, users that do not have Admin privileges can only create the following objects and folders:

- Scorecards
- Scorecard Folders (can only be created in a folder called "User Scorecards")
- Processes
- Process Folders (can only be created in a folder called "My Processes")
- Investor Maps (limited to specified user groups)
- Investor Map Folders (limited to specified user groups and can only be created in a folder called "User Maps")

The permission set for the Owner role for the above objects and folders is as follows:

Folders: Can view existence, read properties, create objects inside this folder, edit properties.

Objects: Can view existence, read properties, edit properties.

C. The "Modules All" User Group

This user group contains all the users who are using a regular ProSight user license. This user group impacts the Modules only (e.g., Investor Maps, Forms, Scorecards, Dashboards, etc.) and is not to be used to control portfolio/data access.

The following specific security rules are applied to this group of users:

- Can use any Module (e.g., Investor maps, Forms, Scorecards, Dashboards, etc.)
- This user group does not affect access to portfolio data. That is handled by the other user groups in this document.

D. The "Modules Forms Only" User Group

This user group contains all the users who are using a ProSight Forms Only user license and is not to be used to control portfolio/data access. This user group impacts the Forms and Investor map modules only. The following specific security rules are applied to this group of users:

VITA Portfolios Security Overview

- Forms Only – This user is not allowed to use any of the Modules except for Forms...
- This user group does not affect access to portfolio data. That is handled by the other user groups in this document.

E. The "000 ITIB" User Group

This user group contains all the users who represent the Information Technology Investment Board. The ITIB is the highest level of approval required for all *Major* Projects and Procurements. The following specific security rules are applied to this group of users:

- View only - all investments and portfolios for all agencies.
- The 000 ITIB group is the only group that can update the data for categories currently named "Approval Entry - ITIB - YesNo", "Approval Entry - ITIB - Comments",
- The 000 ITIB group is denied access to approval processes / portfolios other than their own approval processes / portfolios.
- Can view and create investor maps.

F. The "000 CIO" User Group

This user group contains all the users who represent the Chief Information Officer. The CIO role is the highest level of approval required for all *Non-Major* Projects and Procurements. The following specific security rules are applied to this group of users:

- Can view (read only) all investments and portfolios for all agencies.
- The 000 CIO group is the only role that can update the data for categories currently named "Approval Entry - CIO - YesNo" and "Approval Entry - CIO - Comments" (for Strategic Planning and Baseline approvals) as well as "Approval Proj Status - CIO – Name", "Approval Proj Status - CIO – Phone", "Approval Proj Status - CIO – Email", "Status Report - CIO Approval Comments", "Status Report - CIO Date", "Status Report - CIO – State" (for Project Status approvals).
- The 000 CIO group is denied access to approval processes and portfolios other than their own.
- Can view and create investor maps.

G. The "000 PMD Director" User Group

This user group contains all the users who represent the PMD Oversight Director. The PMD Oversight Director is responsible for setting the "Investment Approval Status". This group has the same privileges as the "000 PMD" Group. The following specific security rules are applied to this group of users:

- Can view and update (read and update) all investments and portfolios for all agencies.
- The 000 PMD Director group is the only group that can update the data for the category currently named "Investment Approval Status".
- Can view and update investment information using all PMD-specific forms (PMD Evaluation, Balanced Scorecard, Service Area Update).
- Can view and update all PMD-specific portfolios (for approvals and locking).
- Can view and update approval indicator categories for all levels of approval.

VITA Portfolios Security Overview

- Can update the categories currently named “Approval Entry - PMD - YesNo” and “Approval Entry - PMD - Comments”.
- Can view and create investor maps.

H. The "000 PMD" User Group

This user group contains all the users who are analysts within PMD. Oversight Director. The PMD Analyst evaluates and reviews investments submitted for approval. The following specific security rules are applied to this group of users:

- Can view and update (read and update) all investments and portfolios for all agencies.
- Can view and update investment information using all PMD-specific forms (PMD Evaluation, Balanced Scorecard, Service Are Update).
- Can view and update all PMD-specific portfolios (for approvals and locking).
- Can view and update approval indicator categories for all levels of approval.
- Can update the data for categories currently named “Approval Entry - PMD - YesNo” and “Approval Entry - PMD - Comments” (for Strategic Planning and Baseline approvals) as well as “Approval Proj Status - PMD – Name”, “Approval Proj Status - PMD – Phone”, “Approval Proj Status - PMD – Email”, “Status Report - PMD Approval Comments”, “Status Report - PMD Date”, “Status Report - PMD – State” (for Project Status approvals).
- Can view and create investor maps.

I. The "000 All Secretariats" User Group

This user group contains all the users who are designated Secretariats within the Commonwealth of Virginia. The Secretariat approves all investments within their domain. The following specific security rules are applied to this group of users:

- Can view (read only) all investments and portfolios for all agencies.
- The 000 All Secretariats group is the only group that can update the data for the “Approval Entry - Sec - YesNo” and “Approval Entry - Sec - Comments” categories (for Strategic Planning and Baseline approvals) as well as “Approval Proj Status - Secretariat – Name”, “Approval Proj Status - Secretariat – Phone”, “Approval Proj Status - Secretariat – Email”, “Status Report - Secretariat Approval Comments”, “Status Report - Secretariat Approval Date”, “Status Report - Secretariat – State” (for Project Status approvals).
- The 000 All Secretariats group is denied access to approval *portfolios* other than their own.
- They are denied access to approval *processes* for PMD, CIO, ITIB.
- Can view and create investor maps.

J. Agency Head User Groups (multiple)

This user group contains all the users who are designated as Agency Heads for their specific agency. The Agency Head approves all investments within their agency. There is one Agency Head User Group for each agency (there are currently approximately one hundred agencies in the Commonwealth of Virginia). The Agency Head User Group name follows the pattern: 999 XXX YYYY AH, where 999 is the agency number, XXX is the secretariat abbreviation and YYYY is the agency abbreviation (e.g. “136 SOTEC VITA AH” is the Agency Head User Group name for VITA). The following specific security rules are applied to this

VITA Portfolios Security Overview

group of users:

- Can view (read only) all investments and portfolios for all agencies.
- The Agency Head group can create / update any investment within their agency (same as the AITR).
- Every Agency Head group is included in the “000 All Agency Heads” user group which is the only group that can update the data for the “Approval Entry - AH - YesNo” and “Approval Entry - AH - Comments” categories (for Strategic Planning and Baseline approvals) as well as “Approval Proj - Agency Head – Name”, “Approval Proj - Agency Head – Phone”, “Approval Proj - Agency Head – Email”, “Status Report - Agency Approval Comments”, “Status Report - Agency Approval Date”, “Status Report - Agency Approval – State” (for Project Status approvals).
- The Agency Head group is denied access to approval *portfolios* other than their own. They are denied access to approval *processes* for Secretariat, PMD, CIO, ITIB.
- Can view and create investor maps.

K. The "000 All Agency Heads" User Group

This group contains every Agency Head User Group and is the only group that can update the data for the “Approval Entry - AH - YesNo” and “Approval Entry - AH - Comments” categories (for Strategic Planning and Baseline approvals) as well as “Approval Proj - Agency Head – Name”, “Approval Proj - Agency Head – Phone”, “Approval Proj - Agency Head – Email”, “Status Report - Agency Approval Comments”, “Status Report - Agency Approval Date”, “Status Report - Agency Approval – State” (for Project Status approvals).

L. AITR User Groups (multiple)

This user group contains all the users who are designated as Agency Information Technology Resources (AITR) for their specific agency. The AITR creates and updates investments for strategic planning within their own agency. There is one AITR User Group for each agency (there are currently approximately one hundred agencies in the Commonwealth of Virginia). The AITR User Group name follows the pattern: **999 XXX YYYY AITR**, where **999** is the agency number, **XXX** is the secretariat abbreviation and **YYYY** is the agency abbreviation (e.g. “136 SOTEC VITA AITR” is the AITR User Group name for VITA). The following specific security rules are applied to this group of users:

- Can view (read only) all investments and portfolios for all agencies.
- The AITR group can create / update any investment within their agency.
- Every AITR group is included in the “000 All AITRs” user group which is the only group that can update the data for the categories currently named “Approval Entry - AITR - YesNo” and “Approval Entry - AITR - Comments”.
- The AITR group is denied access to approval *portfolios*. They are denied access to approval *processes* for Agency Head, Secretariat, PMD, CIO, ITIB.

M. The "000 All AITRs" User Group

This group contains every AITR User Group and is the only group that can update the data for the categories currently named “Approval Entry - AITR - YesNo” and

VITA Portfolios Security Overview

“Approval Entry - AITR - Comments”.

N. Agency User Groups (multiple)

This user group contains all the users who enter new investments and are responsible for maintaining its data throughout the life of the investment. These users are typically project managers or administrative assistants. There is one Agency User Group for each agency (there are currently approximately one hundred agencies in the Commonwealth of Virginia). The Agency User Group name follows the pattern: **999 XXX YYYY Agency**, where **999** is the agency number, **XXX** is the secretariat abbreviation and **YYYY** is the agency abbreviation (e.g. “136 SOTEC VITA Agency” is the Agency User Group name for VITA). In addition to individual users, the Agency User Group contains the corresponding user groups for Agency Head and AITR. This allows a new user to be set up in only one user group based on their role. The following specific security rules are applied to this group of users:

- Can view (read only) all investments and portfolios for all agencies.
- Can create new investments in their respective agency.
- Can update investments where they are named as the “Manager”. If more than one User requires “update” access to an investment, they must be added to the item’s security setting manually by a user in the Administrator group.
- The User role is denied access to approval *portfolios* and *processes*.

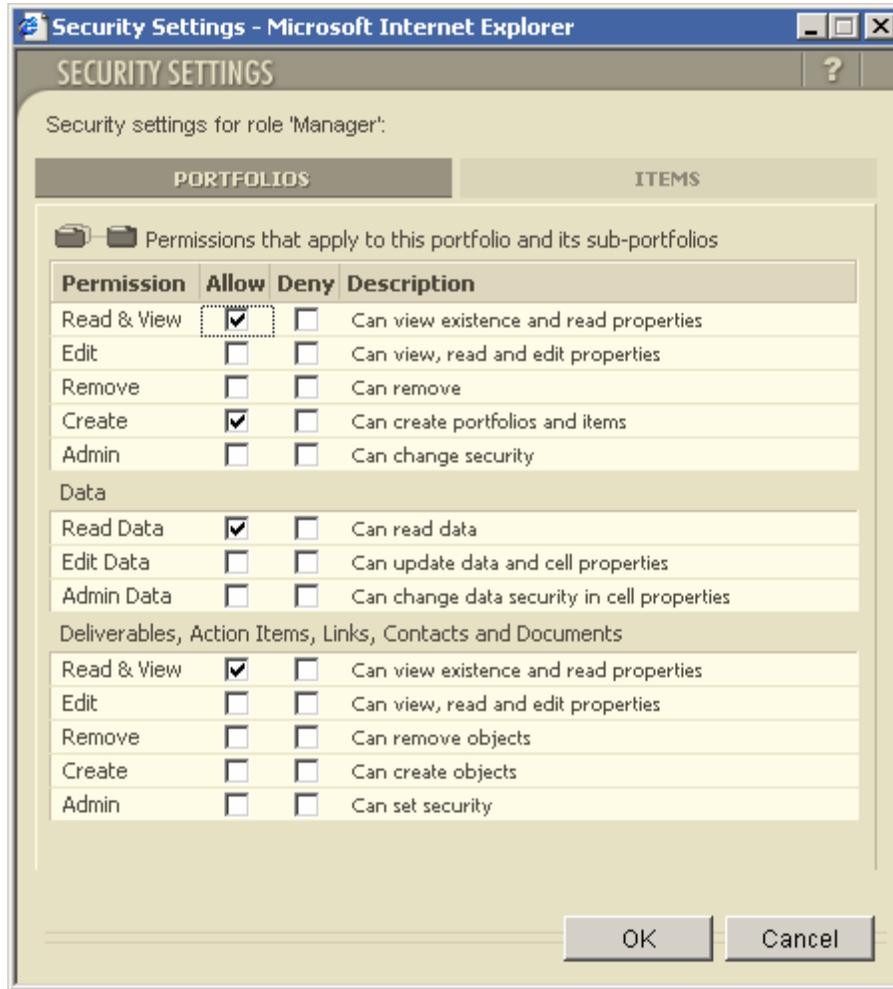
IV. The Closest Permission Sets Win

If there are conflicting permissions for a user group or role, the definition defined closest to the object overrides all others. You can override the parent security policy by either removing the user group or redefining its permission set, or adding new user groups.

V. Allow vs. Deny vs. Do Nothing

Each line in a permission set has a column indicating “Allow” and “Deny”. The setting for any row can either have the “Allow” box checked, the “Deny” box checked, or neither box checked (this is the “Do Nothing” option). The Allow permission overrides the Do Nothing permission. The Deny permission overrides the Allow permission. Here is a sample permission set:

VITA Portfolios Security Overview



VI. Category Security Options

By default, category security is normally defined by the portfolios and the items. This is known as the “inheritance policy”. There are some instances where you want the same security to apply to a category, no matter what the item or portfolio. In these cases you want to change the inheritance policy to "Category defines the security policy (for all Items and Portfolios)". At VITA, there are several “approval” categories that have category security applied. The categories and their corresponding permission sets can be found in the “Details” section of this document.

VII. Using the Manager Role

At Vita, security is currently configured to use the Manager Role. This is accomplished by selecting a user as the Manager of each project. Any user who creates an item, will by default be identified as the Manager of the item. This allows all users in the Agency User Group to read all the items in the portfolios, but only the item Managers will be able to update the data.

Generally speaking, Administrators create all portfolios, so they are the owners of portfolios. The exception to this rule is the individually named portfolios in the “User Portfolios” portfolio. All users can create their own portfolios for their own purposes,

VITA Portfolios Security Overview

but they must reside in the “User Portfolios” portfolio.

VIII. When to Customize Security Permissions

There are times when the standard permission sets don't exactly define the security settings you need. In that case, you can customize any permission set for a user group.

If the user group and permission set is already inherited from a parent, you just need to add the same user group you wish to modify to the security list for the object. Then edit the permission set and check or uncheck the specific permissions you want to change. This will create a custom permission set for this object and any new child objects created under it. For example, if you create a custom permission set for a portfolio, every new portfolio or item created in that portfolio will inherit the custom settings.

IX. Further Information

For complete information on security, refer to the online help or the “ProSight Portfolios User Guide”.