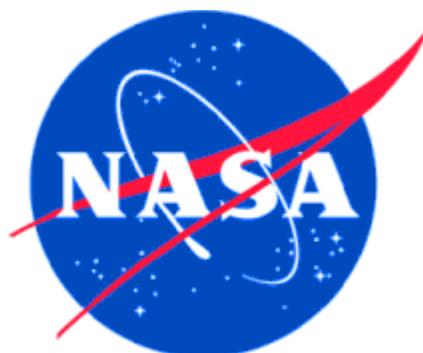# Reuse Enablement System (RES) Policies

Prepared by:
NASA Earth Science Data Systems –
Software Reuse Working Group

March 8, 2010

Earth Science Data Systems Software Reuse Working Group

Editor:

James Marshall (INNOVIM / NASA Goddard Space Flight Center)

Contributing Working Group Members:

Stephen Berrick (NASA Goddard Space Flight Center)

Victor Delnore (NASA Langley Research Center)

Robert R. Downs ** (Columbia University / NASA Socioeconomic Data and Applications Center)

Al Fleig * (PITA Analytic Sciences / NASA Goddard Space Flight Center)

Neil Gerard (INNOVIM / NASA Goddard Space Flight Center)

Larry Gilliam (INNOVIM / NASA Goddard Space Flight Center)

Tommy Jasmin (University of Wisconsin-Madison, Space Science and Engineering Center)

Virginia Kalb (NASA Goddard Space Flight Center)

Louis Kouvaris (Science Applications International Corporation / NASA Goddard Space Flight Center)

Michael Leyton (Rutgers University)

Chris A. Mattmann ** (NASA Jet Propulsion Laboratory)

Shahin Samadi (INNOVIM / NASA Goddard Space Flight Center)

Mark Sherman (SGT Inc. / NASA Goddard Space Flight Center)

Christine Whalen (INNOVIM / NASA Goddard Space Flight Center)

Robert Wolfe * (NASA Goddard Space Flight Center)

* Past Co-chairs

** Present Co-chairs

Working Group Participants:

Nadine Alameh (MobiLaps LLC)

Angelo Bertolli (INNOVIM / NASA Goddard Space Flight Center)

Bradford Castalia (University of Arizona)

Yonsook Enloe (SGT Inc. / NASA Goddard Space Flight Center)

Stefan Falke (Washington University in St. Louis)

Michael Folk (National Center for Supercomputing Applications)

Ryan Gerard (INNOVIM / NASA Goddard Space Flight Center)

Emily Greene (Raytheon Company)

Mary Hunter (INNOVIM / NASA Goddard Space Flight Center)

Gary Jackson (University of Maryland)

David McComas (NASA Goddard Space Flight Center)

Steve Olding (Everware / NASA Goddard Space Flight Center)

Ross Swick (National Snow and Ice Data Center, University of Colorado – Boulder)

Bill Teng (Science Systems and Applications, Inc. / NASA Goddard Space Flight Center)

Curt Tilmes (NASA Goddard Space Flight Center)

Fred Watson (California State University, Monterey Bay)

Jonathan Wilmot (NASA Goddard Space Flight Center)

Table of Contents

1. Introduction

Background

To address the technical issues required to enable and facilitate reuse of software assets within NASA's Earth Science Enterprise (ESE), the NASA Earth Science Software Reuse Working Group was created as part of the Earth Science Data System (ESDS) Working Group. This was the result of one of the recommendations from the NASA HQ-commissioned Strategic Evolution of ESE Data Systems (SEEDS) Study; the SEEDS activity became the ESDS Working Group activity. The Software Reuse Working Group was chartered to oversee the process that will maximize the reuse potential of such software components in order to: (1) drive down the cost and time of system development and reduce/eliminate unnecessary duplication of effort; (2) increase flexibility and responsiveness relative to Earth science community needs and technological opportunities; and (3) increase effective and accountable community participation. The Reuse Enablement System (RES) prototype is a web-based system proposed, designed, and developed by the Software Reuse WG to aid members of the Earth science community in finding and reusing software assets as well as providing their software for others to reuse.

Scope

This policy document defines and recommends the procedures which will be used to govern and administer a RES system. It describes the policies relating to the operation and management of the RES. It outlines the responsibilities and policies related to the normal operation of the RES web site as well as the maintenance of the system. It also defines the activities and provides basic procedures for establishing, operating, and maintaining a software reuse system whether in-house or contracted. This document is not intended to be a requirements or design specification for the RES, nor is it intended to enumerate all applicable privacy policies of the RES.

Document Structure

Following the Application and Supporting Documents and Definition of User Roles sections are the policies developed for the operation and maintenance of the RES. The policy entries are grouped into major categories identified by the chapter headings in the document. Each category contains one or more policy statements, each with three major parts that are formatted as follows:

Policy X#.# – Policy Title

A short statement of the policy.

A longer description of the policy, including any explanatory text.

The first line consists of the word "Policy", the initial(s) of the policy category which is(are) the same as or similar to the name of the section heading under which it is contained, an identifying number for each policy in the form major#.minor#, and a short title that succinctly identifies the policy.

The second part is one or more lines of blue colored text, indented once from the left margin. This section contains a short statement of the policy. Typically this is one or two sentences that concisely state the policy.

The third part is one or more lines of black colored text, indented twice from the left margin. This section contains a longer description of the policy, and may include explanations to clarify points in the shorter statement above.

2. Applicable and Supporting Documents

- Reuse Enablement System (RES) Trade Study (November 17, 2005)

  Author: NASA ESDS Software Reuse WG

- Reuse Enablement System (RES) Use Cases (August 10, 2006)

  Author: NASA ESDS Software Reuse WG

- Reuse Enablement System (RES) Requirements (September 18, 2006, revised May 7, 2007)

  Author: NASA ESDS Software Reuse WG

- Reuse Enablement System (RES) Architecture Study (February 14, 2008)

  Author: NASA ESDS Software Reuse WG

3. Definitions of User Roles

Definition UR1.0 – User Roles

The RES utilizes five groups, each with more privileges than the previous one – Anonymous Users, Consumers, Providers, Content Managers, and Administrators. In addition, other users and/or maintainers of the system may have other relevant roles.

The RES uses "groups" to define the privileges and restrictions placed on users of the site. The term "registered user" applies to Consumers, Providers, Content Managers, and Administrators, all of whom require an approved, registered account on the RES to obtain these user roles. The term "unregistered user" applies to Anonymous Users. Note that registered users who have not logged in to their accounts are treated as Anonymous

Users by the RES. For ease of maintenance and proper collection of statistics, a single user may not have multiple accounts on the RES.

Definition UR1.1 – Anonymous User Role

An anonymous user is any visitor to the web site who has not logged in with a registered account.

Anonymous users only have the ability to search, browse, and view the available download descriptions. They do not have the ability to download any of the assets. They do have the ability to submit comments about the RES to its Administrators.

Definition UR1.2 – Consumer Role

A Consumer is any visitor to the web site who has been approved for a registered account on the RES system.

Consumers are registered users who have all the access rights of anonymous users, but they can also download assets and comment on assets. In addition, they have accounts with the system containing user profiles. This feature allows them to send and receive private messages (PM) within the RES, if it is built using the XOOPS content management system as recommended in the RES Architecture Study, and set (and remove) notifications, which will notify the user by their choice of e-mail or PM of any changes or additions to a certain portion of the system. They also have the ability to modify their account settings (but not their user group), delete their account, show or hide their e-mail address in their profile, and register their usage of an asset in the RES.

Definition UR1.3 – Provider Role

A Provider is a Consumer who has been granted the ability to upload assets to the RES.

The Provider group has the additional privileges of being able to submit their own software assets to the RES, modify other assets within the RES (subject to appropriate approvals), and approve modifications made to assets they have submitted.

Definition UR1.4 – Content Manager Role

A Content Manager is a Consumer or Provider who has been granted limited Administrator privileges for the purpose of administering certain areas (modules) of the RES. Content Managers are responsible for assisting Administrators in managing current and new assets, as well as comments about the system.

Content Managers are tasked with administering the Downloads section of the system, as well as the comments, to verify that assets and comments are relevant and appropriate for inclusion on the RES.

Each category within the Downloads section of the RES may have a dedicated Content Manager(s). These users will be responsible for regulating the assets within the category assigned to them, and providing approval to new assets within that category.

Definition UR1.5 – Administrator Role

An Administrator is a Consumer, Provider, or Content Manager who has full Administrator privileges, providing access to all features of the RES. Administrators are responsible for overseeing the daily operations of the RES and performing tasks such as handling user requests and managing assets.

Administrators have access to a separate administration menu that allows them to create, modify, or delete any user, asset, or element of the system. Administrators also have the ability to create, modify, or delete modules of the system and database entries.

Typical tasks of the Administrator include handling the registration of new users with the system, granting or denying provider access to users requesting it, approving or denying new assets, resolving reports of broken assets, deprecating or masking assets, filtering asset comments, and answering and relaying user comments and questions to the appropriate parties.

Since Administrators have full control of the RES, they need only have an approved, registered account in order to obtain Administrator status (be a Consumer). The privileges of the Provider and Content Manager roles are superseded by the Administrator privileges, so Administrators do not necessarily need to obtain or be granted these roles. While the system only requires one Administrator, it may be beneficial to have more than one, such as for availability reasons (e.g., if one Administrator is on vacation or travel, another one would be available to manage the system).

Summary of Abilities by User Role

Table 1 below provides a summary of the above definitions, showing the basic abilities (system features) each user role has (can use).

Table 1 – Summary of Abilities by User Role

Abilities	Anonymous	Consumer	Provider	Content Manager	Administrator
Search, browse, and view assets	X	X	X	X	X
Send system feedback to Administrators	X	X	X	X	X
Download assets		X	X	X	X
Manage own account		X	X	X	X
Comment on / rate assets		X	X	X	X
Upload / modify assets			X	X	X
Approve modifications to assets			X	X	X
Limited administrator rights, by download category				X	X
Full system administration rights					X

Definition UR2.0 – Other Roles

The RES requires the services of users in roles beyond those in the five user groups utilized by the system for its general user base.

The vast majority of users of the RES will have one or more of the five user roles identified previously. However, as with any computer system, the services of people in other roles besides those of system users is required in order to maintain the system and keep it operating at peak performance. These other roles are described in this section.

Definition UR2.1 – Site Curator Role

Site Curators are responsible for ensuring that the RES web site is available, the RES is operating correctly, and the system is kept up to date.

Typical tasks of the Site Curator, in addition to the above, include creating periodic server back-ups, updating the RES system software, correcting any defects found in the RES, implementing any approved new features or upgrades to the RES, and performing periodic tasks such as ensuring the renewal of the web site domain, the site SSL certificate, etc. The site curator is not tasked with handling requests or issues from RES users.

Definition UR2.2 – NASA ESDS Software Reuse WG Role

The NASA ESDS Software Reuse WG is responsible for assisting Administrators and Content Managers in managing the RES as necessary.

Since the RES is a WG-sponsored activity, the WG leadership (Chair, Co-chair, and Support Team Lead) will discuss any user comments or suggestions forwarded to them by the Administrators, Content Managers, or members of the WG. Through weekly and monthly telecons, the WG leadership will discuss the issue, and decide if a modification to the system or policy should be made, determine the criticality, suggested actions, possible ramifications, and schedule to complete the modifications. The WG leadership will also appoint the Site Curator(s), Administrator(s), and Content Manager(s) as necessary.

4. User Policies

Policy U1.0 – User Statuses

In order to obtain a given user role, users may be required to provide information and/or complete actions commensurate with the level of privileges for the desired role. Any abuse, misuse, or otherwise inappropriate use of the RES may result in the loss of privileges or the loss of the user's account.

The RES requires users to register in order to gain access to software assets and be approved by Administration to upload new assets. Users are placed in a certain group by Administrators according to their requests and background, and any changes to the group of a user will be communicated immediately by e-mail to the user.

Policy U1.1 – Anonymous User Status

All visitors to the RES are automatically granted Anonymous User status.

By definition, anonymous users have not logged in to the RES using a registered account. Therefore all visitors to the RES web site are anonymous users by default. Note that any registered user who visits the site is treated as an anonymous user until he/she logs in to his/her account.

Policy U1.2 – Consumer Status

An Anonymous User may become a Consumer by registering for an account on the RES and having that request approved by an Administrator. Approval is granted if the following conditions are met: a person has registered the account (no automated registrations allowed).

All Consumers must be approved by the Administrators, who have the discretion to deny any registration request.

Policy U1.3 – Provider Status

A Consumer may become a Provider if his/her account is in good standing and he/she can demonstrate the ability to provide useful assets that are relevant to the domain of the RES, and his/her request for Provider status is approved by an Administrator. Approval is granted if the following conditions are met: the user is affiliated with, or has a confirmed reference from someone who is affiliated with, a government agency or educational institution; the user must work in the Earth science domain.

In order to become a Provider, a Consumer must submit a request for Provider status and have that request approved by an Administrator. Consumers wishing to become Providers will complete a provider request form in the RES which asks for their name, official e-mail address, and an optional reference name and contact e-mail. Once submitted, an Administrator will review the information submitted and either grant or deny Provider status to the user.

Policy U1.4 – Content Manager Status

A Consumer or a Provider may become a Content Manager if his/her account is in good standing, he/she has demonstrated expertise in a particular area/field within the domain of the RES, and he/she accepts a request from an Administrator to assist in managing the RES. Approval is granted if the following conditions are met: the user is affiliated, or has a confirmed reference from someone who is affiliated with, with a government agency or educational institution; the user must work in the Earth science domain.

Users are granted Content Manager status by Administrators on a case-by-case basis. Factors in the decision to provide Content Manager status to users may include, but are not limited to: whether the Administrators require additional assistance, what area(s) of the RES would benefit from a Content Manager, whether users are willing to accept the role of Content Manager, and the area of expertise of the users.

Policy U1.5 – Administrator Status

A Consumer, Provider, or Content Manager may become an Administrator if his/her account is in good standing, he/she has demonstrated expertise in managing similar catalog/repository systems, and he/she accepts a request from an Administrator to help manage the RES. Approval is granted if the following conditions are met: the user must be a NASA employee or a contractor directly working on a NASA contract.

Administrator accounts are granted very rarely and on a case-by-case basis by current administrators who are members of the ESDS WG support team or current RES support staff. Factors in the decision to provide Administrator status to users may include, but are not limited to: whether the current Administrators require additional assistance and whether users are willing to accept the role of Administrator.

Policy U2.0 – User Accounts and Groups

The RES limits the number of accounts each user may have, and it controls the roles to which each user belongs.

To assist in operating and maintaining the RES, users are limited in the number of accounts they may have. However, to ensure that they can perform all the actions necessary, they are not limited in the number of roles which they may possess.

Policy U2.1 – User Accounts

Each user is limited to one account.

No user of the RES may have more than one account on the RES system. If any user is found to be in possession of more than one account, the Administrators reserve the right to enforce compliance by means including, but not necessarily limited to, warning the user of the policy violation and requesting that he/she delete extra accounts, or deleting all but one of the user's accounts to force compliance.

Policy U2.2 – User Groups

Users of the RES may belong to more than one of the valid groups in the system.

In most cases, users will only need to be granted the permissions of one user role in the RES. However it is possible, and may be necessary, for a user to belong to more than one role. For example, some Content Managers may serve only in this role, while others may also be either Consumers obtaining assets from the RES or Providers offering assets to the RES for distribution. This is permitted in the RES, and if an Administrator determines it is necessary for a user to belong to more than one role, he/she will modify that user's account accordingly.

5. Downloads

Policy DL1.0 – Downloads

The Downloads section of the RES provides users with the ability to search or browse through a categorized listing of software assets uploaded by other members (alphabetically or hierarchically), review or rate assets, and submit or modify assets. Each user's role determines the privileges he/she will have in the Downloads section.

The RES is built around the Downloads section, the ability to provide reusable software assets, offer feedback about provided assets, and serve as either a software repository (hosting assets locally on the RES) or a simple catalog of assets (providing links to externally hosted assets).

Policy DL1.1 – Creating and Modifying Downloads

Software assets can only be created and/or modified by Providers, Content Managers, and Administrators. The uploader/creator of an asset must have permission to do distribute the asset, and modifications to existing assets require approval of the original Provider and an Administrator.

Providers do not have to be the original author of an asset to submit it. They may submit assets that were either developed by a group of individuals including them, or by other people. However, Providers must first receive permission from the original developers or owners before submitting these assets and credit them appropriately in the download description. Submission will be made by either uploading the asset or by providing a link to the asset, and the Provider will choose which method is used for each asset submitted. The Provider will also be able to categorize each submitted asset, and all assets can be searched for using keywords in their descriptions. In addition, Providers may choose to provide a variety of useful but optional information, such as a checksum for users to use in validating their download of the asset, with each asset submission.

Administrators can modify any user's download through administrator-only pages. Providers can modify their own assets, with the changes taking affect after an Administrator has approved the changes through Administrator-only pages. Providers can only modify other user's assets with both: (a) that user's approval and (b) Administrator approval after original user's approval. If the user is only modifying features of a download, the RES will only update the original download, it should not create a new download or change the submitter name.

Policy DL1.2 – Contributing Assets

Assets contributed to the RES should be tested and prepared for distribution to the general community of Earth science software developers.

All types of assets related to Earth science, at any level of maturity, can be submitted to the RES. However, these assets should not be test versions or other versions for which updates are planned or likely to occur on very short timescales. The RES is not intended to be a vehicle through which developers can test their software. Software should be tested, validated, and verified through relevant and appropriate procedures before being uploaded to the RES. The software should be relatively stable and bug-free, and ready for

distribution to the community. A measure of the asset's maturity in terms of reusability, e.g., through a rating on the Reuse Readiness Level scale developed by the ESDS Software Reuse Working Group, is a beneficial piece of metadata that Providers must specify.

Policy DL1.3 – Linking of Download Versions/Modifications

If a Provider is editing an asset and uploading a new file, the RES will create a new download linked to the old one and deprecate the older one.

The "download history" field will include a listing of links to previous and newer versions of the download with "deprecated" written next to it if deprecated.

Policy DL1.4 – Deprecating Downloads

An asset may be deprecated from the system by a Content Manager or Administrators if the following conditions are met: the original provider requests deprecation; other users request deprecation and the original provider approves of their request.

Deprecating an asset places in bold red, the word "DEPRECATED" in the title of the asset, but it can still be searched for and accessed as the asset remains in the database.

Policy DL1.5 – Suspending Downloads

An asset may be suspended on the system by a Content Manager or Administrators if one of the following conditions is met: feedback has been received that indicates there may be a problem/issue with the asset and an examination/investigation of the asset is required before further action can be taken; the asset Provider requests it and a Content Manager or Administrator approves the request.

Suspending an asset occurs when the permissions on the asset are changed to prevent users from downloading it. This allows the file to remain in the RES and be visible to users (e.g., they can search or browse to find it), but it cannot be downloaded by users. This is intended to be a temporary state that the asset is put into while the examinations/investigations of problem reports are being performed. The asset will be marked as suspended so that users are aware of the situation. The length of time an asset can be marked as suspended is not fixed. The Content Manager or Administrator will consult with the asset Provider, where applicable and if possible, before making deciding whether to suspend the asset.

Policy DL1.6 – Investigating Downloads

Once an asset has been suspended, the Content Manager(s) and/or Administrators will conduct a preliminary examination of the complaint(s) that caused the suspension to determine if a more thorough investigation is required before a decision on how to address the complaint(s) can be made. Decisions on the action(s) to take in order to address the complaint(s) will be made after the preliminary examination if no investigation is required, or after the investigation if it is required.

The investigation of suspended assets takes place in two stages: a preliminary examination and a detailed investigation. The preliminary examination is the first look into the complaint(s) received to determine if a more detailed investigation into the complaint(s)

is required. If an appropriate action can be taken after the preliminary examination, the investigation stops after this first stage, the action taken, and the suspension lifted. Examples of the investigation terminating after the preliminary examination may include when the complaint is found to be unwarranted (e.g., a user is just trying to get an asset taken down) or incorrect (user was mistaken, and the reported problem does not exist). Possible appropriate actions at this stage may include deprecating the asset or dismissing the complaint(s).

If the preliminary examination reveals that further research is required before any action can be taken, the second stage, a detailed investigation, is performed. This is likely to require more time and effort than the preliminary examination, but once it is completed, appropriate actions are decided upon and taken, and the suspension lifted. Possible appropriate actions at this stage may include masking or deleting the download.

Policy DL1.7 – Masking Downloads

An asset may be masked on the system by a Content Manager or Administrators if one of the following conditions is met: the asset has been suspended, an appropriate examination/investigation of the asset has been conducted, and results show that the asset may be stored but not distributed further, the asset has problems that make it not meet its specifications, or the asset has other problems that warrant keeping it in the RES but not allowing users to see or download it; the asset Provider requests it and a Content Manager or Administrator approves the request.

Masking an asset occurs when the permissions on the asset are changed to prevent users from locating, accessing, or downloading it. Masking allows an asset to otherwise remain in the RES. The Content Manager or Administrator will consult with the asset Provider, where applicable and if possible, before making deciding whether to suspend the asset.

Policy DL1.8 – Deleting Downloads

An asset may be deleted from the system by an Administrator if the following conditions are met: the asset has been suspended, an appropriate examination/investigation of the asset has been conducted, and results show that the asset contains a virus, the asset contains inappropriate material, the asset violates RES and/or NASA policies, the asset is masquerading as something it is not, or the asset has similar problems that warrant complete deletion from the RES.

Deleting an asset completely eliminates the asset from the database and removes any file(s) and/or database entries associated with it. Under normal circumstances, this should not be necessary as deprecation or masking should be sufficient to discourage or prevent use of a particular asset. However, the ability to delete assets must exist, for example to remove assets for which the wrong files were uploaded. Because site administration can remove any asset without user notification, users should never use the RES as a single source for storing their personal software. Rather, the system is intended to be used as a catalog/repository for reusable Earth science software, not a backup storage system for critical software components.

Policy DL1.9 – Prioritization of Deprecating, Masking, and Deleting

Under normal circumstances, deprecating is preferred over masking, which is preferred over deleting.

The descriptions provided in DL1.4, DL1.7, and DL1.8 show that deprecating, masking, and deleting form an ordered list of how strong their effects are for users of the RES. Deprecating simply identifies an asset as outdated, but since it remains listed and visible in the system, users are free to use it if they desire. Masking keeps the asset in the system, but prevents it from being visible to users; since users cannot see the asset, they cannot use it, but its record remains in the RES should there be a need to access it in the future. Deleting completely eliminates an asset from the system, and is therefore the most drastic method of limiting or preventing asset usage by RES users; it is also anti-reuse since there is no way to access the asset anymore. Therefore, Administrators and Content Managers must not delete an asset if masking it is sufficient, and they must not mask an asset if deprecating it is sufficient.DL1.5 described suspending assets, which keeps the asset listed and visible in the system, but the asset cannot be downloaded by users. However, this is intended to be a temporary state used while complaints about assets are under investigation. Since it is not designed to be a terminal state, it is not included in the list above, but it is between deprecating and masking in terms of the strength of its effect for users of the RES.

Policy DL1.10 – Right of Administrators to Take Action

The Administrators of the RES reserve the right to decide whether to deprecate, mask, or delete assets when necessary. These actions are subject to the discretion of the Administrators.

In general, Administrators will not deprecate, mask, or delete an asset unless they have approval from the original asset provider. However, there may be times when immediate action is necessary, and waiting for an approval from the original provider is not appropriate. For example, an asset with restricted distribution permissions has been made available without restriction and this must be corrected, or inappropriate material has been uploaded to the system and cannot be allowed to remain. In situations such as these, the RES Administrators reserve the right to take immediate action and deprecate, mask, or delete the asset(s), at their discretion. This decision can be discussed with the original asset provider, and possibly changed, once the need for immediate action has passed, and taking the time to discuss things will not result in more harm than good.

Policy DL1.11 – Reporting Broken Downloads

All users of the RES, regardless of their role, may report the download for an asset they have permission to view as broken.

The IP address of the person reporting the broken link is recorded to help track malicious abuse of the reporting system. The site administration is responsible for periodically checking the system for broken link reports and addressing them, with the assistance of the provider of the asset if necessary. If a broken link report is found to be valid and the original provider cannot be contacted to resolve the issue, the site administration reserves the right to deprecate or remove the asset from the RES.

6. Communications with the Community

Policy C1.0 – Communications with the Community

The RES allows users to communicate with each other and the RES staff through certain pre-defined methods.

Examples of communication methods include providing text comments on assets, providing numerical/quantitative ratings of assets, sending private messages to other users on the system, and sending e-mails to other users who have made their e-mail addresses viewable. Some of these communications, such as text comments and average quantitative ratings, are considered public and will be displayed by the RES for all users to view.

Policy C1.1 – Commenting on Downloads

All registered users may post comments to any asset within the RES that they have permission to view.

Comments are automatically approved, but are regularly monitored by site administration. This may be changed to require approval by a Content Manger or Administrator if deemed necessary. User abuse of commenting rights, such as posting derogatory or inappropriate comments, is a violation of the RES policies. Any such comments will be removed by the administrator..

Policy C1.2 – Rating Downloads

All registered users may rate any asset within the RES that they have permission to view.

Ratings are automatically approved, but are regularly monitored by site administration. User abuses of the rating rights, such as by purposely attempting to influence the overall rating, whether positively or negatively, is a violation of the RES policies. Any such offending rating(s) will be removed by the administrator. The RES will average all such ratings received in order to display an overall rating to users of the system.

Policy C1.3 – Handling User Feedback

Administrators, Content Managers, and Site Curators will monitor all feedback, complaints, suggestions, etc. made by users, and address relevant remarks as deemed appropriate. This may include, but is not necessarily limited to, suspending an asset in order to investigate feedback about it, or updating/correcting asset information/metadata.

Users may submit feedback to the RES Administrators at any point, using the form(s) available on the system. Administrators will monitor this feedback on a regular basis, and respond to it as appropriate. Content Managers and/or Site Curators may need to be involved in the responses as well.

Policy C1.4 – Enforcing Policies

Administrators will take actions as necessary to enforce the policies of the RES. This may include, but is not necessarily limited to, sending warning notices to offending users, banning IP addresses from the system, and deleting user accounts.

The policies of the RES have been created to produce a system that will best serve the reuse purposes of the Earth science community of software developers. Anyone who is found to be in violation of these policies, or otherwise abusing the RES or its users, will be subject to actions taken by the Administrators and/or RES staff. Typically, users will be given at least one warning, and thus a chance to change their behaviour, before more serious measures are taken, such as banning the user's IP address or deleting the user's account.

7. Intellectual Property and Copyrights

Policy IP1.0 – Intellectual Property and Copyrights

All users of the RES must comply with applicable intellectual property rules/laws, copyrights, software licensing agreements, and other similar policies when submitting assets to or using assets from the RES.

Because the RES must allow fast and easy access to Earth Science software assets, Intellectual Property and Copyright issues are inherently a major concern. For the RES to function effectively, providers must be assured that they are not disadvantaging themselves or their organization by submitting software assets. Consumers must be assured that they are within copyright laws when downloading and reusing assets, or possibly selling software that uses components from the RES. Additionally, the RES must comply with all US Copyright laws and NASA policies and directives.

Policy IP1.1 – Providing Content

Providers must have permission to distribute the assets they submit to the RES and must demonstrate this (e.g., by explicitly acknowledging that he/she has this permission, by providing the license under which the asset is released), Providers must also acknowledge that they have read this RES Policies document and agree to its terms.

The uploading of copyrighted and possibly licensed software assets presents challenging intellectual property issues to the RES. Because most content will be developed in an institutional setting, the copyright will most likely belong not to the original creator(s), but to their employing organization or university. Therefore, a non-exclusive rights waiver must be signed by that entity which states that the software may be distributed through the RES, but that the organization still maintains the rights to the intellectual property. Any alternative which demonstrates that the Provider is allowed to distribute the asset(s) being submitted is also acceptable.

Policy IP1.2 – Downloading and Using Content

Registered users must agree to abide by any constraints, restrictions, or license agreement terms that apply to the assets they download from the RES.

Consumers have the right to download any asset from the site and reuse it in part or whole on their projects. However, if the software contains assets listed under certain licenses such as the GNU General Public License (GPL), the Consumer may be obligated to certain conditions, such as making the source of their work available as well. The selling of software products or the use of such software in contracts may be limited based on the licensing associated with the software assets reused.

Policy IP1.3 – Open Source Software

Open source licenses are recommended for assets submitted to the RES.

Software released under an open source license is publicly available and other software developers can read, modify, and redistribute the source code. The WG has recommended greater use of open source licensing, such as the NASA Open Source Agreement (NOSA), as an important enabler for software reuse. The simpler licensing mechanism of open source, compared to traditional software licensing, eliminates a significant barrier to code sharing and thus helps to encourage and promote reuse. Although recommended for assets submitted to the RES, open source licensing is not appropriate for all types of software and therefore traditionally licensed software will also be accommodated.

Policy IP1.4 – NASA Software Release Process

Providers submitting NASA-funded software to the RES must ensure that they have received approval for distribution from their NASA Center's technology transfer office.

At each NASA Center, the Innovative Partnerships Program (IPP) Office and the Software Release Authority (SRA) work together to ensure the proper release of software. Providers submitting any large programs or novel software must first submit a New Technology Report (NTR) to the IPP and receive approval for release under the NASA Open Source Agreement (NOSA) before uploading the software asset to the RES. For more information about the proper software release process at NASA, visit http://www.nasa.gov/offices/ipp/home/index.html.

Policy IP1.5 – Export Controlled Software

The RES will not serve as a repository (locally host) any asset to which access is restricted by export control laws.

The Arms Export Control Act (22 U.S.C. 2778) restricts certain software from being distributed to non-US citizens for defense purposes. The RES currently does not have the ability to host assets that fall under the International Traffic in Arms Regulation (ITAR), Export Administration Regulations (EAR), or any other export control laws, rules, regulations, etc. If such assets are to be included in the RES, they must be hosted on an external site that handles the access controls; the RES will only serve as a catalog for these types of assets, providing links to the external sites hosting them.

8. Privacy and Security of Information

Policy PS1.0 – Privacy and Security of Information

The RES complies with all NASA privacy, security, and accessibility requirements.

The RES complies with all NASA privacy policies and accessibility standards. For more information about these policies, please visit http://www.nasa.gov/about/highlights/HP_Privacy.html. The RES uses session cookies to store all session information. These are only used for login purposes. IP addresses are recorded for all comments to downloads and reporting of broken links to track inappropriate use of the system. We do not divulge any personal information to third parties.

We make every attempt to secure user information and passwords. The RES web site employs Secure Socket Layer (SSL) encryption for all communication between server and client. All user passwords are stored as encrypted 32 character hexadecimal strings in the database. Security tokens are used to validate all web forms that allow modification of user information or user assets.

Policy PS1.1 – Availability of Policies

All policies with which the RES complies will be made available to users.

In order to provide users with detailed information about the policy compliance of the RES, the system will make all policies available to users. Any means by which users are able to access and view these policies, such as via web link to an existing document or by hosting a policy document on the RES itself, will be considered acceptable methods for making the policies available. For the convenience of the users, any location within the RES that providers policies should offer access to all policies (e.g., if a link to NASA policies is included in the footer of the web page, links should also be provided to other policies relevant to the RES so that all policies can be accessed from the page footer).

9. Support for Users

Policy S1.0 – Support for Users

The RES will provide some level of support for its users, which may vary with the user role.

Consumers and Providers in particular may have certain needs for proper and efficient use of the RES, and the RES will provide support to help enable this.

Policy S1.1 – Support for Consumers

The RES will offer as much useful and relevant information about assets as possible.

Consumers need to have as much information as possible about assets in order to make well-informed decisions about which assets are best suited to meet their needs. The RES supports users by providing information such as, but not necessarily limited to, comments on assets, ratings of assets, the ability to contact RES staff, and the ability to contact asset Providers.

Policy S1.2 – Support for Providers

The RES encourages Providers to follow best practices for the assets they submit.

In order to enable software reuse among Consumers, Providers are encouraged to follow best practices in developing and submitting their software to the RES. These may include, but are not limited to, including complete and relevant documentation, providing appropriate packaging and/or installation instructions, and offering test inputs/outputs for verification of program operation.

Appendix A – Glossary

- Accessibility – presenting information in such a way that it can be accessed and used as effectively by users with disabilities as those without.

- Administrator – a user of the RES who controls, operates, and manages the system

- Anonymous user – a user who is not identified by having an account on the RES; an unregistered user. Note that a registered user who does not log in to the RES is treated as an anonymous user.

- Asset – an item produced at some point in the software development life cycle that is recognized as having a particular value

- Browse – the ability or process of manually locating an entry in a catalog or repository, often by navigating through a hierarchy of folders/directories

- Catalog – a system that stores links to assets, but does not store/host the assets themselves

- Consumer – a registered user who is allowed to access or otherwise use assets in the system, subject to their license terms

- Content Manager – a user of the RES whose main role is to review content submitted to the system (e.g., a new asset) for appropriateness and relevance

- Content Management System (CMS) – a program that is used to create the framework for the content of a web site, allowing for convenient management of data files, images, web content, and other material

- Cookies – a piece of text sent by a server to a web browser and then sent back unchanged by the browser each time it access that server

- Copyright – a legal concept that gives the creator of an original work exclusive rights to it, usually for a limited time

- Deprecation – marking a software asset as deprecated, typically to indicate that it has been replaced by a newer version

- Encryption – any method that converts data into a form that cannot be easily understood by unauthorized parties; the reverse method of converting the data back into an easily understood form is decryption

- Intellectual property – creations of the mind; musical, literary, and artistic works are some examples. In the context of the RES, intellectual property refers to the software assets and related artifacts that have been created by its developer(s)

- Intellectual property permissions – the permissions granted to the user of intellectual property by its owner

- Intellectual property rights – the (legal) protections given to the owners of intellectual property

- Internet Protocol (IP) address – a unique address used by electronic devices connected to a computer network using the Internet Protocol to identify and communicate with each other

- License – a document that grants permission to one party by another party. In the context of the RES, this typically refers to the permissions that the developer of a software asset grants to the users of that asset, as defined in an accompanying or referenced license document.

- Portal – a system that serves as a single point of access to varied information and provides a consistent look and feel for accessing that information

- Privileges – a set of permissions on a system that grant a user certain abilities in that system

- Provider – a registered user of the RES who has been granted permission to upload asset resources and metadata to the system

- Registered user – a user of the RES who has completed a registration process in order to obtain an account on the system and been granted an account by an Administrator

- Repository – a system that stores/hosts the actual assets themselves

- Restrictions – any number of rules or exceptions to rules that a user of a software asset must comply with in order to use that asset

- Reusability – the use of existing software, or software knowledge, to build new software.

- Reuse – the integration of a software artifact into another context; a process of implementing or updating software systems using pre-existing software development assets that were created during any part of the software development process. In general, if you have acquired (or used) a software development asset from someplace else that <u>otherwise you would have written yourself</u>, then you have experienced the benefit of reuse.

- Reuse Readiness Level – a set of levels proposed by the NASA ESDS Software Reuse Working Group to measure the maturity level of software in the sense of reusability

- Rights – the power, abilities, permissions, etc. held by the owner of intellectual property

- Rights waiver – the process or document used by the owner of intellectual property to give up one or more of the owner's rights

- Search – the function by which a user may request a listing of all items that match one or more terms

- Security tokens – typically a physical device used in the process of authenticating an authorized user of a system

- Session cookies – a type of cookie that is erased when the user closes the web browser; by contrast, a persistent cookie is one that is retained after the browser is closed

- Submit – refers to the process by which information is provided to the system for inclusion in the system

- Unregistered user – a user who has not completed a registration process in order to obtain an account on the system

- Usability – the ability of a software to be used or how applicable it is to the intended application

- Use – the initial application of a software asset; what the asset was originally designed to do.

- User – any person who accesses the RES

- Virus – a computer program that is able to infect computers, with the user being unaware of the infection, and can replicate itself to infect other computes. This term may also be applied in the more general sense of malware (malicious software that is designed to enter a computer system, possibly to damage it, without the user's informed consent).

- Web site – a collection of Web pages (documents), images, etc. available on the World Wide Web