



Policy and Procedure Manual for the Meteor Network

POLICY AND PROCEDURE MANUAL

Table of Contents

	<u>Page</u>
CHAPTER 1. OVERVIEW.....	1
The Importance of a Policy and Procedure Manual.....	1
Defining Policies and Procedures.....	1
How this Manual is Organized.....	2
CHAPTER 2. THE METEOR NETWORK.....	3
Meteor Users.....	4
Meteor Providers.....	4
The Meteor Federation Model.....	4
Mission Statement.....	7
Vision Statement.....	7
Strategic Objectives.....	7
Critical Success Factors.....	7
Administrative and Operational Organization Chart.....	9
Roles and Responsibilities.....	9
CHAPTER 3. NETWORK POLICIES.....	10
Meteor Advisory Team Participation Policy	10
Network Usage Policy	10
Access Provider Eligibility Policy.....	10
Data Provider Eligibility Policy.....	10
Authentication Agent Eligibility Policy.....	10
Participant Privacy & Security Policy.....	11
Removal from the Network Policy.....	11
Use of Data Policy.....	11
Use of Data Exception Approval Policy.....	11
Disaster Recovery Policy.....	11
Dispute Resolution Policy	11
CHAPTER 4. NETWORK PROCEDURES.....	13
Meteor Registration Process – Access Providers.....	13
Meteor Registration Process – Data Providers.....	15
Meteor Registration Process – Authentication Agents.....	16
New Participant Review Procedure.....	17
Authentication Level Setting Procedure.....	18
Production Problem Reporting and Resolution Procedure.....	19
Code Donation Review and Distribution Procedures.....	20
APCSR Alias List Review Procedure.....	21
Meteor Registry Change Procedures.....	22
Removal from the Network Procedure	23

Use of Data Exception Procedure.....	24
Source Code Change Procedure.....	25
Security Breach Reporting Procedure.....	26
Dispute Resolution Procedure.....	27

Chapter 1. OVERVIEW

The Importance of a Policy and Procedure Manual

Most organizations today recognize the value of having a policy and procedure manual that governs the general operations and fiscal practices of the organization. The Meteor™ Advisory Team (MAT) has created this Policy and Procedure Manual to go beyond governance and to systematically address all aspects of the Network operations. Administering a Network such as Meteor is complex, and written policies and procedures contribute to the long-term stability and safety of the Network by:

- **Providing documentation of the Network's vision and operating principles**

This Policy and Procedure Manual provides a clear statement of the mission, values, and vision of the Network and provides the framework that defines the Network's operating principles and processes.

- **Providing staff with clear guidelines on how to administer a program**

This Policy and Procedure Manual provides detailed, step-by-step instructions on how the Network is administered and clearly defines roles, expectations, and routine operating guidelines.

- **Addressing risk management issues**

This Policy and Procedure Manual is fundamental to risk management of the Network because it provides clear and explicit instructions on how every part of the Network is administered. This allows Network participants and administrators to *safely*, *effectively*, and *consistently* manage the Network.

Defining Policies and Procedures

Policies and procedures represent the sum total of foundational decisions, requirements, and activities needed to run the Network. All major program operations are captured in the following policies and procedures. For purposes of clearly defining the Network's operating principles, the following classifications are made:

Policies

Policies are high-level program statements that embrace the goals of the Network and define *what* is acceptable to ensure success and effective, consistent program operations. Policies are crucial to achieving the Network's mission and goals and are developed for program practices that are mandatory and non-negotiable in nature. Policies lower the risk of program failure and reduce the threat of legal recourse. Policies may indicate who has authority for final decisions and broad consequence options for non-compliance. Policies are approved and monitored by the MAT.

Procedures

Procedures are statements that describe *how* a particular operational function is to be implemented and managed within the Network. Procedures are brief statements that describe the step-by-step process necessary to implement and support the Network's policies and practices. Procedures include descriptions of who is responsible for each task. Procedures are governed by the MAT.

Comparison of Policies and Procedures

Policies	Procedures
Widespread application	Narrower focus
Non-negotiable, changes infrequently	Open to change or continuous improvement
Expressed in broad terms and requirements	Detailed descriptions of activities
Statements of “what” and/or “why”	Statements of “how,” “when,” and/or “who” and sometimes “what”
Answers major operational issue(s)	Describes process
Approved by MAT	Managed by the MAT and contract staff

How This Manual Is Organized

The purpose of this manual is to provide an overview of the Network’s policies and procedures. The contents of this manual include all policies and procedures necessary to the successful operation of the Network.

Chapter 1. Overview

This chapter provides general information about the importance of policies and procedures as well as an overview of the structure of the manual.

Chapter 2. The Meteor Network

This chapter includes essential information about the Network. This information is important because it helps to define and outline the core structure of the Network and the MAT.

Chapter 3. Network Policies

This chapter identifies core critical policies that the Network uses to *administer* the Network.

Chapter 4. Network Procedures

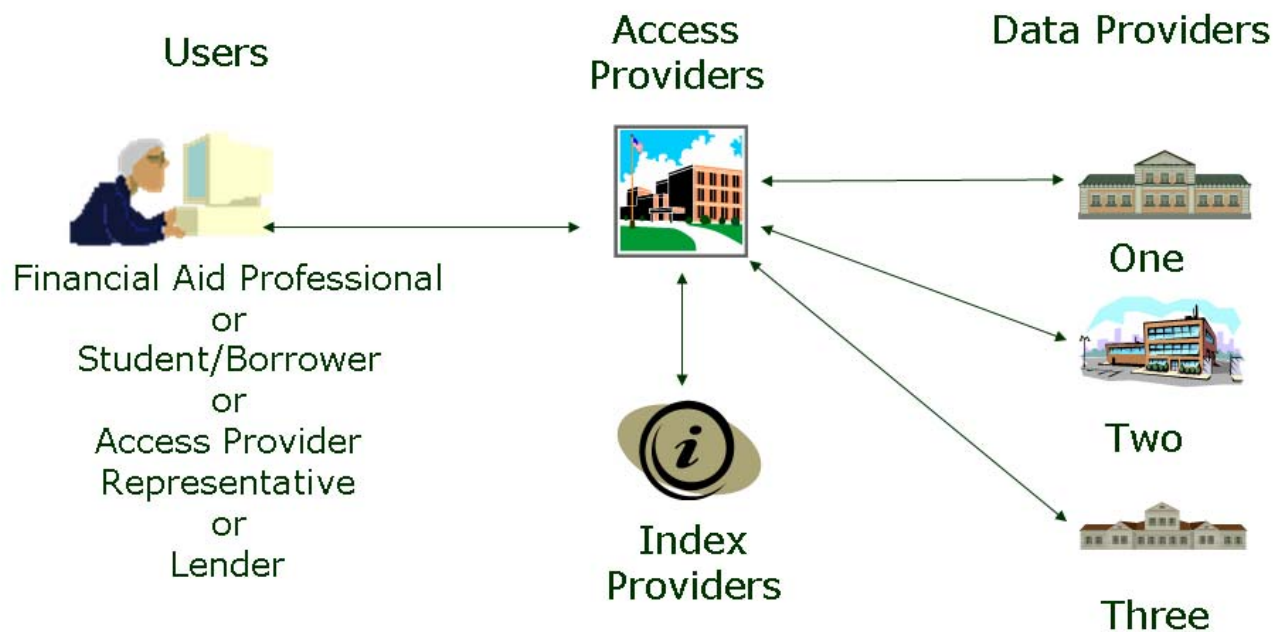
This chapter addresses the Network procedures that *support* and *operationalize* the Network policies.

Chapter 2. THE METEOR™ NETWORK

The Meteor software provides a web-based universal access channel to student/borrower financial aid information. The Meteor Software displays aggregated financial aid award information for FEELP and alternative loans. Future implementations are planned to include Perkins loans, Federal Direct loans, grants, scholarships and other financial aid awards. The current Meteor Network aggregates student/borrower loan information for display to Financial Aid Professionals, students/borrowers, and customer service professionals. Meteor Access Provider customer service representatives have the ability to view data on student aid to which their organization is a party. The Meteor software is provided by the FEELP industry as a gift to schools and students/ borrowers. The National Student Clearinghouse is leading this effort as another collaboration of industry participants, to provide quality products to schools and students/borrowers.

The objective of the Meteor Network is to provide accurate and comprehensive information to Financial Aid Professionals to help them with counseling students/borrowers and assisting with the financial aid process in general. The Meteor Network also provides accurate and comprehensive information to students/borrowers to assist them in tracking their financial aid history. It is also designed to assist customer service professionals at Access Provider locations with assisting Network users.

The Meteor Process



Meteor Users

There are four types of user in the Meteor Network:

- Students/Borrowers
- Financial Aid Administrators
- Customer Service Representatives
- Lenders

Meteor users have varying levels of access to information provided within the Meteor Network. These distinctions will be made throughout this guide, as appropriate.

Meteor Providers

Providers within the Meteor Network are broken down into four fundamental categories: Access Providers, Data Providers, Authentication Agents and Index Providers.

A Meteor Access Provider hosts a copy of the Meteor Access Provider software. Access providers can be schools, guarantors, lenders, servicers, or secondary markets. After performing its own authentication of the user making the inquiry, the Meteor Access Provider software generates a request to the appropriate Data Providers for the student/borrower's information. The software uses an index to identify the location(s) of the requested student/borrower financial aid information and thereby creates efficiencies in the request process.

A Meteor Data Provider hosts a copy of the Meteor Data Provider software that enables them to respond to an Access Provider's request for information. Data Providers are typically lenders, servicers, guarantors, and secondary markets.

A Meteor Authentication Agent is an organization that creates an assertion attesting to the fact that a user is who they claim to be. The Authentication Agent can be a school, guarantor, lender, servicer or other organization that has a database of information on individuals sufficient to validate an end users identity.

A Meteor Index Provider hosts a copy of the Meteor Index Provider Software that allows them to identify the Data Providers for which the Access Providers need to contact on a student-by-student basis. Because there is no central database within Meteor, the Index Provider serves as the central source for information on the location of a student's financial aid information. The Meteor Network is designed to support multiple Index Providers, as there is no single source of ALL financial aid information available in Higher Education.

The Meteor Federation Model

The Meteor Network provides organizations with a federated authentication methodology. This enables providers to easily implement enhanced web services without requiring bilateral agreements. The Meteor Network providers agree to follow the policies and procedures of the Network. This results in multilateral trust among all providers. The Meteor Network thereby builds a framework for widespread authentication and identity management within the higher education community.

The Meteor Network has created a set of business rules that define the minimum requirements for participation and to address organizational liabilities. This information can be found in the Meteor Participant Certification document.

A fundamental critical success factor in Meteor acceptance and for widespread adoption is the integrity of the network. This means that Data Providers, Access Providers, students/borrowers, schools, and auditors must be confident that Meteor meets reasonable requirements for data privacy and security. Accordingly, Meteor has established the following security and privacy objectives:

- Comply with the Gramm-Leach-Bliley Act (GLBA), Department of Treasury interagency guidelines, and other state enacted legislation and be able to pass an independent audit for Security and Privacy;
- Assure Data Providers that reasonable authentication mechanisms are used so that only authenticated inquirers have access to the network;
- Assure Data Providers that appropriate authority levels will be used to control what data an inquirer is enabled to view, based on their role, authority, and relationship to the data (data filtering);
- Perform the above with a minimum level of administrative overhead and intrusive requirements for schools, students/borrowers, Access Providers and Data Providers; and
- Provide a flexible foundation for future Meteor enhancements that will allow additional functions to be added without causing major changes in the authentication and privacy infrastructure.

In order to meet these objectives, the Meteor effort developed an authentication model that is supported by a number of industry standards. The following design principles are incorporated in this model:

- Digital Certificates will be used to authenticate Access Providers and Data Providers, and
- The OASIS SAML XML security standard is used. Internet 2 “Shibboleth” authentication architecture was used as a model for Meteor technical standards. You can obtain more information on Shibboleth at <http://shibboleth.internet2.edu/>

The Access Provider performs authentication of inquirers using their current login rules that establish the initial level of authentication. Data Providers will be able to identify the authentication process used by the Access Provider or Authentication Provider in the case of third party authentication through the Meteor registry entry for that Access Provider or Authentication Provider.

- If the Data Provider requires a more stringent or “higher level” of authentication than the Access Provider or Authentication Provider has performed, then the Data Provider may require that an additional authentication request be solicited from the inquirer (e.g., Data Provider requires a private password or PIN which is a more stringent or “higher level” of authentication than the student/borrower name and date of birth authentication performed by the Access Provider or Authentication Provider).
- If a higher level of authentication is obtained, then the entity providing that authentication must sign the new authentication assertion and Data Providers will use that new higher level of authentication instead of the initial level of authentication as a comparison against their required level.

Electronic authentication (E-authentication) is the process of establishing confidence in user identities electronically presented to an information system. The National Institute of Standards and Technology (NIST) have published recommendations to provide technical guidance to allow an individual person to remotely authenticate his/her identity to a Federal IT system, *Electronic Authentication Guideline*, [[NIST 800-63](#)]. This guidance addresses only traditional, widely implemented methods for remote authentication based on secrets. With these methods, the individual to be authenticated proves that he or she knows or possesses some secret information. NIST expects to explore other means of remote authentication (for

example using biometrics, or by extensive knowledge of private, but not truly secret, personal information) and may develop additional guidance on the use of these methods for remote authentication. The Meteor Advisory Team continually monitors state and Federal authentication standards to ensure that the Network is in compliance with the latest trends in security and authentication.

This technical guidance supplements OMB guidance, *E-Authentication Guidance for Federal Agencies*, [OMB 04-04], that defines four levels of authentication Levels 1 to 4, in terms of the consequences of the authentication errors and misuse of credentials. Level 1 is the lowest assurance and Level 4 is the highest. The OMB guidance defines the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides Federal agencies with the criteria for determining the level of e-authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence of each application or transaction.

The NIST recommendations state specific technical requirements for each of the four levels of assurance in the following areas:

- *tokens* (typically a cryptographic key or password) for proving identity,
- *identity proofing*, registration and the delivery of credentials which bind an identity to a token,
- *remote authentication mechanisms* -- that is, the combination of credentials, tokens and authentication protocols used to establish that a claimant is in fact the subscriber he or she claims to be, and
- *assertion mechanisms* used to communicate the results of a remote authentication to other parties.

NIST defines Level 1 authentication as authentication with no identity proofing requirements and provides a low level of assurance that the user is who they claim to be. Plaintext passwords or secrets are not transmitted across a network at Level 1

NIST defines Level 2 authentication as a model that provides single factor remote network authentication. At Level 2, identity-proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2. It allows any of the token methods of Levels 3 or 4, as well as passwords and PINs. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay, and on-line guessing attacks are prevented.

Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated by the Credentials Service Provider (CSP); however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are required. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

The Meteor Network is compliant with the NIST Level Two authentication guidelines.

More detail regarding authentication is contained in *Section 2, Technical Reference* of the Meteor Implementation Guide available at www.meteornetwork.org.

Mission Statement

Meteor will be recognized and accepted as the standard for real time, secure access to comprehensive, timely and accurate student financial aid information.

Vision Statement

Meteor will be THE standard means for accessing higher education data from distributed sources.

Strategic Objectives

- I. *Objective:* Provide, through open collaborative participation, freely available open-source software and support that enables low cost implementation.
- II. *Objective:* Provide the right data at the right time from the right source.
- III. *Objective:* Continue to be an open source product collaboratively developed by industry participants, which embraces recognized and emerging technology standards to provide for quick secure access to distributed data.
- IV. *Objective:* Enable participants to provide their customers with real-time access to comprehensive financial aid data anytime and anywhere.
- V. *Objective:* Secure all-inclusive implementation by data and access providers.

Critical Success Factors (CSF)

For each objective, we have identified specific critical success factors for meeting the objective.

- I. ***Objective: Provide, through open collaborative participation, freely available open-source software and support that enables low cost implementation.***
 - A. Sufficient high quality human resources to support and enhance Meteor must be consistently available.
 - B. MAT ensures evaluation of industry issues and perspectives.
 - C. Provide high quality technical support.
 - D. Sufficient financial resources to support the strategic objectives.
- II. ***Objective: Provide the right data at the right time from the right sources.***
 - A. 100% of the FFELP data.
 - B. Ensure best source of data.
 - C. Ensure that data presentation meets the needs of the end users.
 - D. Provide access to state, federal, institutional financial aid and private loan data.

III. Objective: Continue to be an open source product collaboratively developed by industry participants, which embraces recognized and emerging technology standards to provide for quick secure access to distributed data.

- A. Sufficient high quality technical human resources to support and enhance Meteor must be consistently available.
- B. Provide a forum to research and implement emerging technologies.
- C. Participate in industry standard setting initiatives.
- D. Maintain/enhance software development and testing infrastructures.
- E. Maintain the highest level of integrity and security.
- F. Provide a version of the Meteor software for those participants whose organizations prohibit usage of Open Source software.

IV. Objective: Enable participants to provide their customers with real-time access to comprehensive financial aid data anytime and anywhere.

- A. Provide end user documentation (e.g. online help and user guides are KPIs)
- B. Provide network availability 24/7 and fast response time.
- C. 100% of FFELP data.
- D. Ensure timely reporting and updating to the index and registry.
- E. Minimize implementation steps for access providers and data providers.
- F. Limit number of releases per year and ensure they are backward compatible.
- G. Continue to support a customizable look and feel.
- H. Maintain and enhance participant support infrastructure.
- I. Ensure that data presentation meets the needs of the end users.
- J. Conduct periodic end user surveys through the access provider.

V. Objective: Secure all-inclusive implementation by data and access providers.

- A. Schools should see the value in using Meteor to drive increased participation.
- B. Meteor is seen as value added to existing services offered by organizations rather than a threat.
- C. Meteor is viewed as a value added service to be provided by access providers and data providers to their customers.
- D. Meteor obtains safe harbor from DE.
- E. Meteor members and participants must see a return on investment.
- F. Maintain the highest level of integrity and security.
- G. Meteor must build alliances with other industry organizations in order to gain industry acceptance.

The Meteor Network

CHAPTER 3. METEOR™ NETWORK POLICIES

Meteor Advisory Team Participation Policy

It is the policy of the Meteor Network that membership on the Meteor Advisory Team (MAT) is limited to individuals employed by Meteor Member organizations. There will be certain instances, however, when specialized teams may need to be formed with participation outside of the MAT. In these instances, the MAT will have responsibility to approve such requests.

Network Usage Policy

It is the policy of the Meteor Network that all users of the Network must be authenticated by an Access Provider or Authentication Agent prior to being given access to data on the Network. Refer to the Meteor Conditions of Use and the Meteor User Certification information contained in the Meteor Participant Certification document.

The Access Provider or their Authentication Agent is responsible for ensuring that the end-user is eligible to use the Network and for assigning and determining the role of the end-user. The Participant organizations will support the project manager in these activities as required.

Access Provider Eligibility Policy

It is the policy of the Meteor Network that all Access Providers meet the requirements and agree to the terms of the Meteor Participant Certification document.

The MAT assumes lead responsibility for the determination of eligibility for participation.

Data Provider Eligibility Policy

It is the policy of the Meteor Network that all Data Providers meet the requirements and agree to the terms of the Meteor Participant Certification document.

The MAT assumes lead responsibility for the determination of eligibility for participation.

Authentication Agent Eligibility Policy

It is the policy of the Meteor Network that all Authentication Agents meet the requirements and agree to the terms of the Meteor Authentication Agent Certification document.

The MAT assumes lead responsibility for the determination of eligibility for participation as an Authentication Provider.

Participant Privacy & Security Policy

It is the policy of the Meteor Network that all participants have established policies, procedures and practices to protect against unauthorized access to, or use of, data received through their Meteor Network connection. It is also the policy of the Meteor Network that participants agree to promptly report to the MAT any individuals whom the Meteor Participant believes may be improperly obtaining data through the Meteor Network. It is the policy of the Meteor Network that all participants meet and adhere to the requirements set forth in the Meteor Participant Certification document.

The Meteor Participants certify their compliance with the participant privacy and security policy. The MAT is responsible for the monitoring of participant compliance.

Removal from the Network Policy

It is the policy of the Meteor Network that a Meteor Participant may withdraw from participation in the Network by providing at least thirty (30) days advance written notice to the MAT. Additionally, the MAT may revoke participation in the Network without notice, in cases where the integrity of the Network is at risk.

The project manager assumes lead responsibility for the coordination of removal of participants from the Network under the direction of the MAT. The Participant organizations will support the project manager in these activities as required.

Use of Data Policy

It is the policy of the Meteor Network that Meteor Participants shall not capture, store, use or reuse any data obtained through the Meteor Network. This prohibition does not apply to postsecondary school Participants so long as the use is in connection with the Participant's official duties. Additionally, no Meteor Participant shall use any data obtained through the Meteor Network for marketing and/or solicitation purposes.

The Meteor Participants certify their compliance with the use of data policy. The MAT is responsible for the monitoring of Participant compliance.

Use of Data Exception Approval Policy

It is the policy of the Meteor Network that a Meteor Participant shall be allowed to capture, store, use or reuse any data obtained through the Meteor Network so long as the Participant demonstrates to the MAT that it will only use the data for one of the purposes identified in the Meteor User Certification.

The MAT assumes lead responsibility for the granting of exceptions to the Use of Data policy. Clearinghouse staff and Board of Directors will support the MAT in these activities as required.

Disaster Recovery Policy

It is the policy of the Meteor Network that all Network participants and providers have a disaster recovery plan that identifies and mitigates against risks to critical systems and sensitive information in the event of

a disaster. These plans shall provide for contingencies to restore information and systems if a disaster occurs.

The MAT assumes lead responsibility for ensuring that all participants and providers have sufficient plans in place.

Dispute Resolution Policy

It is the policy of the Meteor Network that, should disputes regarding Network services or the use of those services arise among Participants or between a Participant and the Network, the participants should follow the appropriate procedures for resolving the dispute.

Upon resolution, a brief description of the dispute issues and the resolution of those will be posted to the members-only section of the Meteor website.

The MAT assumes lead responsibility for dispute resolution. Clearinghouse staff and Board of Directors will support the MAT in these activities as required.

CHAPTER 4. METEOR™ NETWORK PROCEDURES

Meteor Registration Process – Access Providers

Purpose The purpose of this procedure is to outline the registration process for a potential Meteor Access Provider.

Process The following table outlines the registration process for a potential Meteor Access Provider.

Step	Action
1	Potential Access Provider (AP) contacts Meteor Registration Coordinator (MRC) at meteor@studentclearinghouse.org
2	Potential AP should obtain the following from the MRC: <ul style="list-style-type: none"> • Meteor Participant Certification • Registration Profile • Authentication Profile(s) • Technical Profile
3	Potential AP should complete all forms from Step 2.
4	Potential AP submits completed forms, along with a copy of their Authentication Policy to the MRC at: Meteor Registration Coordinator c/o The National Student Clearinghouse 2300 Dulles Station Blvd, Suite 300 Herndon, VA 20171 Note: If AP is using an Authentication Agent, then they must submit the name of the agent as well as the Authentication Policy of that agent. The AP does not need to complete the Authentication Profile, but must submit an Authentication Profile for its agent.
5	MRC emails completed forms and Authentication Policy to the Meteor Team Leads.
6	The Meteor Team Leads review the documents and assigns appropriate authentication level.
7	The MRC contacts the Meteor registry host to designate the potential AP as “active” in the test registry and to update the authentication level of the provider.
8	The MRC contacts the potential AP and advises them to contact the Meteor Index Provider, the National Student Clearinghouse (Clearinghouse), to begin connectivity testing.
9	Potential AP contacts the MRC upon successful completion of testing.
10	The MRC contacts the Meteor registry host to designate the new AP as “active” in the production registry.
11	The MRC coordinates all announcements and press releases with the new AP.

12	The MRC updates the following: <ul style="list-style-type: none">• The Meteor website with new AP as an active participant• The Meteor business production listserv with AP's primary business contact• The Meteor technical production listserv with AP's primary technical contact
13	Process ends

Meteor Registration Process – Data Providers

Purpose The purpose of this procedure is to outline the registration process for a potential Meteor Data Provider.

Process The following table outlines the registration process for a potential Meteor Data Provider.

Step	Action
1	Potential Access Provider (DP) contacts Meteor Registration Coordinator (MRC) at meteor@studentclearinghouse.org
2	Potential DP should obtain the following from the MRC: <ul style="list-style-type: none"> • Meteor Participant Certification • Registration Profile • Technical Profile
3	Potential DP should complete all forms from Step 2.
4	Potential DP submits completed forms to the MRC at: Meteor Registration Coordinator c/o The National Student Clearinghouse 2300 Dulles Station Blvd, Suite 300 Herndon, VA 20171
5	MRC emails completed forms to the Meteor Team Leads.
6	The Meteor Team Leads review the documents.
7	The MRC contacts the Meteor registry host to designate the potential DP as “active” in the test registry as well as the appropriate minimum authentication level accepted. Any other pertinent information should also be updated in the registry at this time.
8	The MRC contacts the potential DP and advises them to contact the Meteor Index Provider, the National Student Clearinghouse (Clearinghouse), to begin connectivity testing.
9	Potential DP contacts the MRC upon successful completion of testing.
10	The MRC contacts the Meteor registry host to designate the new DP as “active” in the production registry.
11	The MRC coordinates all announcements and press releases with the new DP.
12	The MRC updates the following: <ul style="list-style-type: none"> • The Meteor website with new DP as an active participant • The Meteor business production listserv with DP’s primary business contact • The Meteor technical production listserv with DP’s primary technical contact
13	Process ends

Meteor Registration Process – Authentication Agents

Purpose The purpose of this procedure is to outline the registration process for a potential Meteor Authentication Agent.

Process The following table outlines the registration process for a potential Meteor Authentication Agent.

Step	Action
1	Potential Authentication Agent (AA) contacts Meteor Registration Coordinator (MRC) at meteor@studentclearinghouse.org
2	Potential AA should obtain the following from the MRC: <ul style="list-style-type: none"> • Authentication Agent Certification • Registration Profile • Authentication Profile(s) • Technical Profile
3	Potential AA should complete all forms from Step 2.
4	Potential AA submits completed forms, along with a copy of their Authentication Policy to the MRC at: Meteor Registration Coordinator c/o The National Student Clearinghouse 2300 Dulles Station Blvd, Suite 300 Herndon, VA 20171
5	MRC emails completed forms and Authentication Policy to the Meteor Team Leads.
6	The Meteor Team Leads review the documents and assigns appropriate authentication level.
7	The MRC contacts the Meteor registry host to designate the potential AA as “active” in the test registry and to update the authentication level of the provider. Any other pertinent information should also be updated in the registry at this time.
8	The MRC contacts the potential AA and advises them to complete testing with their Access Providers.
9	Potential AA contacts the MRC upon successful completion of testing.
10	The MRC contacts the Meteor registry host to designate the new AA as “active” in the production registry.
11	The MRC coordinates all announcements and press releases with the new AA.
12	The MRC updates the following: <ul style="list-style-type: none"> • The Meteor website with new AA as an active participant • The Meteor business production listserv with AA’s primary business contact • The Meteor technical production listserv with AA’s primary technical contact
13	Process ends

New Participant Review Procedure

Purpose The purpose of this procedure is to outline the review process for prospective new participants.

Process The following table outlines the review process for new participants

Step	Action
1	The Meteor Advisory Team (MAT) Teams Leads receive a new participant certification request from an organization
2	MAT Team Leads assess the following regarding the organization: <ul style="list-style-type: none">• Are they a member of the community• Purpose of their participation• Intended use of the data• Assigned OPEID – If the participant does not have an OPEID or a NCEHLP assigned id, the registration coordinator will work with NCHELP to obtain a NCHELP assigned id for the participant.
3	MAT Team leads review whether or not a customized display is requested, if so, the MAT team leads will follow the Use of Data Exception Procedure.
4	If all of the above are found to comply with Meteor policy the registration process continues as per the participation role(s) requested (Access Provider, Data Provider, and/or Authentication Agent).
5	If any of the above does not to comply with Meteor policy, the organization is notified by the registration coordinator that the request is denied with an explanation of the reason for denial.

Authentication Level Setting Procedure

Purpose The purpose of this procedure is to outline the review process for determining the appropriate authentication level to be assigned to the Access Provider or Authentication Agent.

Process The following table outlines the review process for new participants.

Step	Action
1	The Meteor Access Provider or Authentication Agent should submit the Authentication Profile along with a detailed explanation of how their authentication process works to the Meteor registration coordinator.
2	The Meteor registration coordinator reviews the documentation for completeness.
3	If complete, the registration coordinator disseminates the documentation to each of the team leads
4	Independently, each team lead reviews the documentation and assigns an authentication level (Refer to the Meteor Implementation Guide for a description of each level of authentication supported in the Meteor Network). Each reviewer forwards their determination to the registration coordinator If anyone determines there is not sufficient information to make an authentication determination the lead will inform the registration coordinator of the type of additional information need from the participant
5	If all leads assign the same level of authentication, the authentication level is set to that level; If all leads do not assign the same level, the registration coordinator will schedule a conference call for the leads to discuss the respective level assignments and to work toward building consensus on the level of authentication to be assigned.
6	Notification – The Meteor registration coordinator will notify the participant of the level assigned.
7	The meteor registration coordinator will then follow the new registry procedures to complete the process.

Production Problem Reporting and Resolution Procedure

Purpose The purpose of this procedure is to identify the troubleshooting procedures as well as the production problem reporting and resolution procedures.

Process The following table outlines the process for reporting and resolving production problems.

Step	Action
1	A Meteor access or data provider identifies a potential problem with the performance of the Meteor software.
2	IT resources from the access or data provider determine if the organizations servers and applications are performing correctly.
3	Access or Data Provider IT resource verifies that Meteor is successfully connecting to their systems.
4	If the Access or Data Provider determines their servers, applications and connections are functioning properly, the Access or Data Provider IT resource sends an email and any supporting documentation to the Meteor help desk.
5	The Meteor helpdesk will run through a series of trouble shooting activities to try and isolate the problem.
6	If the Meteor helpdesk cannot determine the cause of the problem, the helpdesk staff will contact the Meteor developer for assistance.
7	If a problem is identified with the provider, the Meteor help desk contacts the provider to inform them of the problem and recommended actions that will be required to resolve the problem.
8	If a software problem is identified, the Meteor helpdesk will open a problem ticket.
9	If a network problem is identified, the helpdesk will open a problem ticket. If the problem is affecting the entire network, the helpdesk will send an email to both the Meteor business and technical production listserves with a cc: to the MAT and MAT tech-team listserves.
10	Problem tickets will be reviewed by the MAT and the Meteor developer to determine possible solutions to the problem reported.

Code Donation Review and Distribution Procedures

Purpose The purpose of these procedures is to outline the process for the review, acceptance and distribution of any code donated to the Meteor project.

Process The following table outlines the process for the review, acceptance and distribution of the donated code.

Step	Action
1	Determine if the code donation is an enhancement to the current production code or if it fixes a bug in the current version or in a previous version.
2	If the code donation is an enhancement, the functionality must be reviewed and approved by the MAT. The change and the approval must be documented as a use case or issue paper and recorded in the Meteor documentation site. If the code donation fixes a bug, the donating organization must document the problem and how it was resolved tying the documentation back to the bugtraq numbers. It is recommended that the donating organization also include the xml (or the information that is triggering the condition) for test cases when available.
3	Donating organization coordinates with the MAT Technical Team Lead to have the code and change log posted to the Meteor Technical Sharepoint site.
4	Business/Technical team reviews the problem reported and the solution created and makes a determination on the impact of the bug, the change, and how and when the revised code will be implemented.
5	Donating organization walks through the code changes with the business team, the tech team and the Meteor project developer.
6	Tech team and Meteor project developer review the changes made [.] to validate that the code modifications correct the problem reported and does not impact the code in any other way.
7	MAT determines if the donated code is acceptable as submitted or if additional changes should be made. If the donated code is acceptable, the MAT authorizes the Meteor project developer to incorporate the changes into a new build of the software.
8	The MAT determines the testing requirements and sequence.
9	Business team builds test cases as appropriate. Technical team builds test cases as appropriate.
10	Business and technical testing of the Meteor code.
11	Upon successful completion of testing, user documentation is revised as appropriate, notification to organizations currently in production, development, and/or testing is delivered, and the implementation-tracking matrix is updated as appropriate.

APCSR Alias List Review Procedure

Purpose

The purpose of this procedure is to outline the process for the review and maintenance of the APCSR alias lists.

Process

The following table outlines the process for the review and updating of the Meteor registry in support of the APCSR alias lists.

Adding, deleting or changing the status of registry records:

Step	Action
1	APCSR Access Provider submits a registration profile form which lists the OPEID's for which their customer service staff is eligible to view information. The profile must be returned along with the certification that a contractual agreement between the APCSR AP and the owner(s) of the data to which access will be granted is in place.
2	The Meteor registration coordinator reviews the organization OPEID's and/or NCHELP issued data exchange ids, and the profile document.
3	The Meteor registration coordinator verifies the codes are valid codes.
4	The Meteor registration coordinator contacts the data owner(s) to confirm access to the APCSR Access Provider and provides them with an APCSR Acknowledgement Form for signature.
5	Data owner(s) review, sign, and return Acknowledgement Form to the Meteor registration coordinator.
6	If approved, the Meteor registration coordinator forwards the alias list(s) to the Meteor registry host for inclusion in the central registry.
7	If not approved, the Meteor registration coordinator responds back to the Access Provider with an explanation. At this point, the Access Provider may submit additional documentation to bring the code to approval.

Meteor Registry Change Procedures

Purpose The purpose of this procedure is to outline the process for changing the production registry for a Meteor provider.

Process The following tables outlines the process:

Adding, deleting or changing the status of registry records:

Step	Action
1	Meteor Provider contacts Meteor Registration Coordinator (MRC) at meteor@studentclearinghouse.org
2	Meteor Registration Coordinator confirms the change with the Meteor Team Leads.
3	Meteor Registration Coordinator approves the change and sends the provider data to the Meteor Help Desk at meteorhelpdesk@studentclearinghouse.org .
4	The Meteor Help Desk makes the change and emails notification to the Meteor Registration Coordinator that the change has been made.
5	The Meteor Help Desk will connect to the failover registry provider to ensure that any changes propagate successfully to the replicated registry.
6	If changes do not propagate successfully, the Meteor Help Desk will work with the failover registry provider to ensure successful replication.
7	Process ends.

Updating public key data for existing registry records:

Step	Action
1	Meteor Provider emails their new public key to the Meteor Help Desk at meteorhelpdesk@studentclearinghouse.org .
2	Meteor Help Desk contacts the Meteor Provider and verifies the fingerprint of the key.
3	Meteor Help Desk deletes the previous key and adds the new key to the provider's registry record(s).
4	The Meteor Help Desk notifies the provider that the change has been made.
5	The Meteor Help Desk will connect to the failover registry provider to ensure that any changes propagate successfully to the replicated registry.
6	If changes do not propagate successfully, the Meteor Help Desk will work with the failover registry provider to ensure successful replication.
7	Process ends.

Updating contact information for existing registry records:

Step	Action
1	Meteor Provider emails their new contact information to the Meteor Help Desk at meteorhelpdesk@studentclearinghouse.org .
3	Meteor Help Desk updates the provider's registry record(s).
4	The Meteor Help Desk notifies the provider and the Meteor Registration Coordinator that the change has been made.
5	The Meteor Help Desk will connect to the failover registry provider to ensure that any changes propagate successfully to the replicated registry.
6	If changes do not propagate successfully, the Meteor Help Desk will work with the failover registry provider to ensure successful replication.
7	Process ends.

Removal from the Network Procedure

Purpose The purpose of this procedure is to outline the process for removing an existing member from the Meteor Network. This procedure will outline two distinct types of removals -- voluntary and involuntary. A voluntary removal will be when a member needs to stop participating for some reason. An involuntary removal will be when a member must be removed to protect the Meteor Network.

Process The process is outlined in the following steps:

Step	Action
Voluntary Removal:	
1	Member notifies Meteor Project Manager at least 30 days prior to requested removal date that they intend to discontinue participation in the Meteor Network. A date and time are agreed to.
2	The Meteor project manager notifies all Meteor members via the email groups, of the member's request and expected date and time to depart.
3	Project Manager schedules the removal from the Meteor Registry with the Registry Host.
4	Project Manager works with Registry host to assure and test the removal takes place as planned.
Involuntary Removal:	
1	Meteor receives notification of a breach of agreement or other security problem pertaining to a Meteor member.
2	Project Manager is immediately notified.
3	Project Manager makes determination to remove the offending member. They may have discussions with other members and/or offending member.
4	Project Manager notifies Registry Host to remove the offending member from the Meteor Registry ASAP.
5	Project Manager works with the registry host to test to ensure the offender was removed.
6	Project Manager notifies Meteor Network via email groups.

Use of Data Exception Procedure

Purpose

The purpose of this procedure is to outline the review process for allowing and exception to the data use policy.

Process

The following table outlines the review process for exceptions to the data use policy:

Step	Action
1	The Meteor Project Manager or the Meteor Advisory Team (MAT) Team Leads receives a request for an exception to the data use policy.
2	MAT Team Leads assess the following regarding the request: <ul style="list-style-type: none">• Purpose of their participation• Intended use of the data
3	MAT Team Leads review whether or not a Customized display is requested or not? <ul style="list-style-type: none">• If not, ok.• If yes, collaborative approach on development with MAT
4	If the use exception is approved, the Meteor Project Manager will inform the participant the request is approved.
5	If the use exception is not approved, the Meteor Project Manager will inform the participant the request has been denied.
6	The Meteor Project Manager and Clearinghouse legal counsel will review any requests that are proprietary.

Source Code Change Procedure

Purpose The purpose of this procedure is to outline the approval process for source code changes.

Process The following table outlines the approval process for source code changes:

Step	Action
1	Business requirements are developed by the Meteor Advisory Team in conjunction with the Meteor Software Developer.
2	The business requirements will be documented by the Meteor Software Developer, reviewed and refined accordingly by the MAT.
3	A formal signoff on the requirements document will be required by the Meteor Project Manager, MAT Business Team Lead and the Meteor Software Developer prior to the code phase beginning. The signoff phase will include a development estimate by the Meteor Software Developer.
4	Coding phase, unit testing and automated regression testing
5	Upon completion of the unit testing and auto regression a build will be available for business team and tech team testing.

Security Breach Reporting Procedure

Purpose

The purpose of this procedure is to outline the process for Meteor participants to report security breaches and what action will be taken by the Meteor team.

Process

The following table outlines the process for Meteor participants to report a security breach and the appropriate actions to be taken by the Meteor team.

Step	Action
1	Upon identification of a material breach, any Meteor participant must promptly report the breach to the Meteor Help Desk and terminate their connectivity to the network immediately.
2	The Meteor Help Desk will de-activate the Meteor participant in the Meteor registry – production and failover.
3	The Meteor Help desk notifies MAT team leads and project manager.
4	The MAT team leads and project manager will review and assess the situation and communicate to network participants as necessary.
5	Depending on the severity of the breach, if the MAT team leads determine that the Network should be shut down, appropriate steps will be taken to shut down the production registry and index as well as the failover environments. The Meteor project manager will communicate as necessary to organizations in production.
6	The MAT will work with the provider to correct the breach and restore connectivity.
7	The MAT team leads and project manager will communicate updates to the Network participants as necessary.

Dispute Resolution Procedure

Purpose The purpose of this procedure is to outline the dispute resolution process between participants and among participants and the Network.

Process The following table outlines the dispute resolution process for Meteor Network participants.

NOTE: This procedure will evolve as the MAT gains more experience with the types of disputes that may occur.

Step	Action
Disputes Among Participants	
1	Participants should make every reasonable effort to settle disputes among themselves, especially if contractual issues are involved. . However, if circumstances warrant, then the Meteor team leads may be asked to act as arbitrator in helping the participants come to resolution.
2	The Meteor project manager will gather as much information as possible from each disputing party and share this information with the Meteor team leads.
3	The team leads and project manager will hold a conference call to review the information (requesting additional information as necessary).
4	The Meteor project manager will offer the proposed solution to the disputing parties.
5	If this process fails to bring consensus among the participants, then the dispute should be escalated to a dispute between participants and the Network. (See process below.)
6	If this process brings consensus among the participants, the participants will take the appropriate steps to implement the solution.
Disputes Between Participants and the Network	
1	Any participant may submit a written request to the Meteor project manager with regard to aspect of the operation or services supported by the Network.
2	The project manager will validate that sufficient information has been provided to define the dispute and will notify the MAT team leads.
3	The team leads will appoint one of the members to serve as the mediator with the disputing party(s).
4	The mediator will collect all the facts and rationales for the dispute and, as necessary, seek advice from other relevant parties.
5	The mediator will prepare a report which will include a recommended resolution of the dispute. The report shall be submitted to the project manager within 30 days unless delayed due to fact-finding requirements.
6	The project manager will share the report with the team leads. The team leads may require additional information or a modified recommendation after reviewing the report.

7	Resolution of the dispute must be approved by affirmative vote of the team leads. If the team leads are unable to affirm a resolution, the status quo is maintained.
8	The project manager shall report the team lead's action to the disputing party(s) in writing.