



***For use in the Electronic Procurement Project
Known as the "Multi-State E-Mall"™***

The Current Version of this Document is Available at
<http://e-mall.osd.state.ma.us/or>

Copyright © 1998 by the Commonwealth of Massachusetts in its capacity as Policy Authority for the Multi-State E-Mall. All rights reserved. Permission to reproduce this document is hereby granted provided that the following limitations on this right are observed: (1) all copies must clearly indicate that this work is published by and attributed to the Commonwealth of Massachusetts in its capacity as Policy Authority for the Multi-State E-Mall; and (2) all copies must include this notice of copyright.

file:///Users/DazzaHomeFolder/Desktop/Email/oprules-v1.htm (1 of 19) [3/27/11 9:32:00 PM]

A. Scope

A.1. General

A.2. Application of these Operating Rules

A.3. Open Buying on the Internet

A.4. Contact Information

B. Authentication: In General

B.1. Issuance, Use, Modification and Termination of User Name and Passwords

B.2. Use of SSL

B.3. Use of S/MIME

B.4. Use of Fax, Telephone, U.S. Mail, Commercial Couriers, and Unsecured/Unauthenticated E-Mail

B.4.1. General

B.4.2. Communication of Agreements and Related Data

B.4.3. Other Communications

C. Authentication: Certificate Policy

C.1. Introduction

C.2. General Provisions

C.3. Identification and Authentication

C.4. Operational Requirements

C.5. Physical, Procedural, and Personnel Security Controls

C.6. Technical Security Controls

C.7. Certificate and CRL Profiles

C.8. Specification Administration

D. Roles, Functions and Authorization of Participating Parties

D.1. General Concepts

D.2. Role: Policy Authority (E-Mail Team/Principal)

D.3. Role: Business Administrator (E-Mail Team/Admin.)

D.4. Role: Operations Administrator (E-Mail Team/Admin.)

D.5. Role: State Partner MOU Signatory (State Partner/Principal)

D.6. Role: State Coordinator (State Partner/Contact)

D.7. Role: Shopper (State Partner/User)

D.8. Role: Operational Approver (State Partner/User)

D.9. Role: Financial Approver (State Partner/User)

D.10. Role: Receiver (State Partner/User)

[D.11. Role: Supplier Partner MOU Signatory \(Supplier Partner/Principal\)](#)

[D.12. Role: Supplier Coordinator \(Supplier Partner/Contact\)](#)

[D.13. Role: Certificate Manufacturer](#)

[D.14. Role: Solution Providers](#)

[E. Technical Requirements](#)

[E.1. User Personal Computer](#)

[E.1.1. Internet and World Wide Web Connectivity](#)

[E.1.2. Hardware](#)

[E.1.3. Software](#)

[E.2. Supplier Partner](#)

[E.3. Physical Security of Computing and Network Resources](#)

[F. Duties and Obligations of the Parties](#)

[F.1. Electronic Offer and Acceptance](#)

[F.1.1. OBI Order Request](#)

[F.1.2. OBI Order](#)

[F.2. Notice](#)

[F.3. Participation Agreements](#)

[F.4. Confidentiality](#)

[F.5. Intellectual Property](#)

A. Scope

A.1. General

The Multi-State E-Mall Pilot (E-Mall) is an Extranet procurement Web site, hosted by the Commonwealth of Massachusetts and available to participating states. The E-Mall web site provides links to qualified supplier "storefronts" or catalogs, where state procurement staff can browse, shop and create requisitions. Public Key Certificate technology coupled with user name and password ensure that only authorized procurement staff can submit approved OBI Orders to the approved suppliers.

A.2. Application of these Operating Rules

These Operating Rules apply to every participant in the E-Mall. No party may play any role or otherwise act as a participant in the E-Mall without signing a Participation Agreement. Depending on the role a given party plays

(i.e. User, Supplier, Administrator, etc.) a different Participation Agreement with special terms may be required.

A.3. Open Buying on the Internet

The E-Mall is based upon the Open Buying on the Internet (OBI) specification. OBI is an emerging standard that defines the technical requirements for conducting business over the Internet from buyer to seller.

The following definition is copied from the OBI web site:

The OBI standard is an open, flexible design for business-to-business Internet commerce solutions. It is intended for the high-volume, low-dollar transactions that account for 80% of most organizations' purchasing activities. Version 1.0 of the standard document contains an architecture, as well as technical specifications and guidelines. OBI is not a product or a service; it is a freely available standard which any organization can obtain and use.

Information about the OBI standard is available at the website <http://www.openbuy.org>. Version 1.0 and Version 1.1 of the OBI technical specifications are available from this site.

A.4. Contact Information

The Policy Authority promulgating these Operating Rules is the Commonwealth of Massachusetts. A current version of these Operating Rules and related information is available at <http://e-mall.osd.state.ma.us/> or. Signed Participation Agreements of each party performing a role under these Operating Rules are on file with the Policy Authority. For purposes of business communications, parties performing a role in the E-Mall may contact:

Nancy Burke, E-Mall Project Manager,
Commonwealth of Massachusetts, Operational Services Division
One Ashburton Place, Room 1017
Boston, MA 02108
nancy.burke@state.ma.us, 617.727.7500

For questions or comments specifically relating to these Operating Rules, parties performing a role in the E-Mall may contact:

Daniel Greenwood, Deputy General Counsel, Information Technology Division & E-Mall Steering Member
Commonwealth of Massachusetts
One Ashburton Place, Room 801
Boston, MA 02108
dan.greenwood@state.ma.us, 617.973.0071

B. Authentication: In General

B.1. Issuance, Use, Modification and Termination of User Name and Passwords

A Username and Password must be supplied by every User of the E-Mall Server accessing a non-public portion of the system. No User may share or otherwise reveal their Password. Any suspicion that a Password has been compromised must be immediately communicated to the State Coordinator for that user. A Password may be re-set in the event that an authorized user forgets the Password. Upon proper notification by an authorized State Coordinator under these Operating Rules and relevant implementing agreements, a User access to the E-Mall will be terminated and the respective Username and Password combination for a terminated User will no longer be valid.

B.2. Use of SSL

Every person accessing any non-public portion of the E-Mall server must use the Secure Sockets Layer (SSL) protocol. The SSL protocol will be used to authenticate and secure certain communications between Supplier servers and the E-Mall server as well as to encrypt certain session between the browser of a user and the E-Mall server and authenticate the identity of authorized E-Mall users. A web session invoking version 3.x of the SSL protocol requires use of a duly issued Public Key Certificate within the browser of an E-Mall user.

B.3. Use of S/MIME

A Pilot Participant who is duly issued a Public Key Certificate for use in the E-Mall may use that Certificate to "sign" e-mail to another participant. In addition, a Pilot Participant may use the duly issued E-Mall Certificate of another participant to encrypt e-mail using the S/MIME standard, provided each person uses an interoperable e-mail client. In some cases, as determined by an E-Mall Administrator, use of S/MIME may be requested or required to assure official communications via e-mail are confidential and/or authenticatable.

B.4. Use of Fax, Telephone, U.S. Mail, Commercial Couriers, and Unsecured/Unauthenticated E-Mail

B.4.1. General

Access as a User or Administrator to the E-Mall server will require a valid Username and Password as well as a recognized Public Key Certificate. However, many other communications channels will be used for various

other purposes throughout the term of this pilot. It is recognized that implementation of a production system will require greater specificity regarding permitted and prohibited methods of communication and corresponding authentication depending on the purposes of the communications. It is intended that experience gained through this pilot process will demonstrate appropriate guidelines. For purposes of the pilot, however, it is expected that most non-critical communications will occur between pilot participants via phone and e-mail.

B.4.2. Communication of Agreements and Related Data

Communication of the implementing agreements under these Operating Rules and related User designation and authorization data requires greater specificity. Until and unless otherwise specified in future versions of these Operating Rules, delivery of all completed forms, agreements and related data, including all designation of roles and authorities for users of the E-Mail system must be communicated via:

- * Fax, U.S. Mail or Commercial Couriers, or

- * Upon prior approval by the E-Mail Business Coordinator, S/MIME Signed E-Mail, signed by private key corresponding to a validly issued Public Key Certificate for the E-Mail Pilot

Until and unless return receipt is received by phone call back or other agreed methods, sender must consider that such data has not been successfully transmitted.

B.4.3. Other Communications

Unless otherwise specified in these Operating Rules, communications may be conducted by any reasonable means that are appropriate for the purpose.

C. Authentication: Certificate Policy

For purposes of the Multi-State E-Mail Pilot, a Public Key Certificate is a computer-based record which:

- (a) identifies the entity or brand associated with issuance of it;
- (b) names or identifies the person or device associated with the corresponding private key;
- (c) contains the public key corresponding to that private key of that person or device; and
- (d) is digitally signed by the Certificate Manufacturer that creates the Certificate.

In transacting business over the Internet, it is critical that both the seller and buyer be assured that the transactions exchanged are secure. Public key encryption coupled with Public Key Certificates can

provide part of this security by ensuring the confidentiality and/or authentication of electronic business exchanges. When Public Key Certificates are attached to transactions, users on each side of a purchase can be assured of who the message came from and that it was not tampered with. The E-Mall pilot uses Certificates to bolster the authentication provided by the Password and Username in the E-Mall system. A Certificate is not, by itself, sufficient to gain access or perform any transactions within the E-Mall system.

Public Key Certificates are used to authenticate Web servers and their clients via protocols such as SSL 3.0. A Public Key Certificate is analogous to an identification card issued by a third party. Each User participating in the E-Mall pilot must have at least one Public Key Certificate. Certificates will be issued at no cost by a designated and trusted third party known as a Certificate Manufacturer (CM). The CM will issue a Certificate to Users who have been identified by their respective State Coordinators and accepted by the E-Mall Administrator.

The browser specifications as noted in the technical requirements' section accommodates the use of Public Key Certificates.

A technical resource for each State Partner will be needed to install the Certificates for each user. This technical resource must have an adequate understanding of the technical, operational and legal requirements and responsibilities associated with managing, issuing and maintaining Public Key Certificates.

This Certificate Policy section of these Operating Rules governs creation, delivery and other aspects of the Certificate Manufacturing process as well as the proper use of Public Key Certificates. This section follows the format of the Internet Engineering Task Force PKIX Part 4 Framework (available at <http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part4-03.txt>) and is in general accord with the guidance provided by Version 1.0 of the draft "Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates" by the Certificate Authority Ratings and Trust Task Force of the Internet Council of the National Automated Clearinghouse Association (available at <http://internetcouncil.nacha.org/CARAT/>).

NOTE: The public release of Version 1.0 of these Operating Rules will not contain the Certificate Policy due to concern for maintaining control over disclosure of information revealing sensitive security processes. Parties that have a need to know some or all of the information contained within the Certificate Policy may request such information from the Policy Authority. For the purpose of indicating the general form and scope of the Certificate Policy, certain section headings have not been redacted, but no content will be published under any heading in this section.

C.1. Introduction

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

C.2. General Provisions

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

C.3. Identification and Authentication

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

C.4. Operational Requirements

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

C.5. Physical, Procedural, and Personnel Security Controls

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

C.6. Technical Security Controls

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

C.7. Certificate and CRL Profiles

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

C.8. Specification Administration

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

D. Roles, Functions and Authorization of Participating Parties

D.1. General Concepts

Party: A legal entity. A natural person can be a party. Certain organizations, such as corporations, trusts and governments may also be recognized as a legal person and therefore can be a party.

Each party will be identified by name in relevant documents and agreements.

Functions: The particular duties and obligations entered into within a business and technical system. A Party will perform several functions. These sets of functions are put together based on technical, legal and business needs of the enterprise.

Role: Each *role* is named according to the nature of the functions in each set. By naming roles, and associating functions with roles, it is not suggested that in every business model sets of functions will be divided in the same manner as here. Further, it is not suggested that there will be one-to-one correlation between roles and parties. Indeed, it is envisioned that a *party* may perform one or more roles. The purpose for naming roles in this document is primarily to provide a vocabulary for creating modular parts that can be perform by a given party entering the E-Mall system and to organize the obligations and related documents associated with a given party.

For example, rather than call the administration role by the name Commonwealth of Massachusetts, it is convenient to name it based on the relevant suite of functions so that any party could perform the role more easily within the system of documents and business arrangements herein. Similarly, while particular parties perform the role of service providers, there may be additional and/or different parties playing those roles in the future, hence we use terms like "solution provider" and "Certificate Manufacturer." The usage of roles under these Operating Rules is intended to reflect and support the potential evolution of this project from a relatively closed and small pilot to a scalable production system in which many more parties may perform the roles noted herein.

Documents and Agreements: In many cases, a party will have to sign a document or submit a particular form as part of the functions associated with a given role. These documents might be contracts, memoranda of understanding, applications, reports and so on. These documents hold a particular legal importance as the glue that hold together parties, roles and functions in a predictable and enforceable system.

D.2. Role: Policy Authority (E-Mall Team/Principal)

Functions

- * Sponsor of the Multi-State E-Mall Pilot;
- * Makes all policy decisions related to the Multi-State E-Mall Pilot;
- * Designates, and delegates appropriate authority to E-Mall Administrators;
- * Agrees to accept the MOU of State Partners; and

- * Selects and arranges for technology products and services necessary for hosting the E-Mall OBI-Compliant server on behalf of State Partners as buying organizations.

Relevant Documents and Agreements

- * Promulgates, or delegates authority to promulgate, these **Operating Rules** and all other official agreements or documents related to the Multi-State E-Mall.

D.3. Role: Business Administrator (E-Mall Team/Admin.)

Functions

- * Receives names/contact data of each State Coordinator from each designated Partner State (from person(s) who signed the MOU);
- * Gives the State Coordinator contact information to the Operations Administrator;
- * Reviews and submits for processing all security related applications and forms, including those related to Public Key Certificates, which are forwarded by the State Coordinator; and
- * Securely maintains all applications and forms for related Public Key Certificate requests before and after processing by the E-Mall Operations Administrator.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Must sign **Business Administrator Agreement**.

D.4. Role: Operations Administrator (E-Mall Team/Admin.)

Functions

- * Responsible for administering the E-Mall servers, including the IEC Server and the Database Server;
- * Responsible for creating and/or amending and/or terminating user accounts and related user authorizations on E-Mall system in accordance with instructions from authorized E-Mall State Coordinators; and
- * Responsible for requesting Certificate Manufacturer to create and deliver a Certificate to each authorized user.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Must sign **Operations Administrator Agreement** governing authorization rights and responsibilities to the E-Mall Server and related matters.

D.5. Role: State Partner MOU Signatory (State Partner/Principal)

Functions

- * Agrees to be an E-Mall Pilot Participant by signing the State MOU;
- * Designates the authorized Coordinator for the participating state government; and
- * Sponsors a Supplier for participation in the E-Mall with a valid, current contract with that state.

Relevant Documents and Agreements

- * Signs the **State MOU** that includes reference to agreement with policy materials (herein known as these **Operating Rules**).

D.6. Role: State Coordinator (State Partner/Contact)

Functions

- * Primary Operations and Business point of contact for communications with E-Mall Administrators;
- * Designates state users and their respective authorization rights, including designation as a Shopper, Approver, or Receiver;
- * Assists users in application process and with use of the E-Mall system;
- * Designates authorized Supplier Partner(s); and
- * Immediately notifies the E-Mall Operations Administrator of changes in authority (including termination) for any user.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**. Signs **State Coordinator Agreement** and **User Designation and Authorization** forms for each authorized user.

D.7. Role: Shopper (State Partner/User)

NOTE: The role of Shopper is also known as "Requisitioner" for certain technical purposes within the I.E. C. application and the E-Mall system.

Functions

- * May shop on and through the E-Mall system;
- * Must use system only for authorized purposes and not use Public Key Certificate for any non-E-Mall pilot purpose;
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, the Shopper will:
 - * shop available E-Mall catalogs on the Web to determine best value;
 - * select a participating Supplier;
 - * access the Supplier's storefront (electronic catalog) with contracted pricing in the E-Mall;
 - * select items to be purchased;
 - * create an OBI Order Request with the Supplier;
 - * verify in-house inventory availability as appropriate;
 - * adjust the OBI order request as necessary; and
 - * complete the OBI Order, flagging the OBI Order for operational approval.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.8. Role: Operational Approver (State Partner/User)

Functions

- * May shop and must process approved OBI Orders created by other Shoppers;
- * No Approver may approve an OBI Order that they placed themselves unless they have been specifically authorized by the appropriate personnel at their state and that authorization has been successfully communicated to the E-Mall Administrator by the Approver's Sate Coordinator (note: this exception will be approved in appropriate circumstances, such as when a user works in a one person departments);
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, the Operational Approver will:

- * review the OBI Order Request;
- * adjust the OBI Order Request as necessary; and
- * approve or deny the OBI Order Request on-line, flagging the OBI Order for Financial Approval.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.9. Role: Financial Approver (State Partner/User)

Functions

- * May shop and must verify that the appropriate "encumbrance" and payment related financial controls for their state have been satisfied and documented;
- * This role may be combined with the Operational Approver;
- * Must enter relevant "legacy system" encumbrance and payment related numbers into the E-Mall system;
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, and /or the legacy accounting system as appropriate, the Financial Approver will:
 - * verify funds availability;
 - * process an encumbrance in the legacy accounting system known as: legacy system;
 - * cross-reference the legacy system encumbrance and OBI Order Request for audit purposes and release the detailed OBI Order for EDI 850 Transmission;
 - * review and adjust invoices submitted for payment electronically in the EDI 810 format through the E-Mall
 - * process payment in the legacy accounting system known as: legacy system;
 - * update payment information on the OBI Order;
 - * financial approval must ensure that an appropriate legacy system entry has been made before an OBI Order is sent to the Supplier.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.10. Role: Receiver (State Partner/User)

Functions

- * Must indicate in the system when commodities shipped as a result of an E-Mall OBI Order have been received in full and/or part, making notations as appropriate concerning the exceptions noted at the time of delivery;
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, the Receiver will:
 - * physically accept and verify commodities received;
 - * record receipt of commodities in the E-Mall.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.11. Role: Supplier Partner MOU Signatory (Supplier Partner/Principal)

Functions

- * Makes catalogs available according to the OBI specification as implemented for E-Mall through the E-Mall Operating Rules;
- * Is an authorized Supplier for purposes of doing business with participating E-Mall Partner States.
- * Accepts the E-Mall server Certificate and their own approved server Certificate as a secure, authenticated and binding method of transmitting quotes, orders (also known as OBI Order Requests and OBI Orders) through the E-Mall system, as specified under these Operating Rules;
- * Designates Supplier Coordinator.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **Supplier MOU** and the **Electronic Commerce Supplier Partner Agreement**.
- * Signed respective **contracts** with the sponsoring state pursuant to applicable procurements laws for purposes of doing business with that state.

D.12. Role: Supplier Coordinator (Supplier Partner/Contact)

Functions

- * Primary Operations and Business point of contact for E-Mall communications with the Supplier Partner.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.

D.13. Role: Certificate Manufacturer

Functions

- * Creates Public Key Certificates as requested by E-Mall Operations Administrator;
- * Creates said Certificates according to the Certificate profile specified by E-Mall Policy Authority;
- * Abides by the Certificate Policy section of these Operating Rules governing creation, delivery and other aspects of Certificate Manufacture as documented agreed by the Policy Authority, following the format of the Internet Engineering Task Force PKIX Part 4 Framework (available at <http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part4-03.txt>) and in accord with the general guidance provided by Version 1.0 of the draft "Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates" by the Certificate Authority Ratings and Trust Task Force of the Internet Council of the National Automated Clearinghouse Association (available at <http://internetcouncil.nacha.org/CARAT/>).

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**, including the **Certificate Policy**, and warrants that any internal documented practices, such as a Certificate Practice Statement, are consistent with these Operating Rules and Certificate Policy.
- * Signs **Certificate Manufacturer Agreement**.

D.14. Role: Solution Providers

Functions

- * Provide products and services necessary for State Partners to conduct OBI-Compliant transactions via the E-Mall;
- * Conduct initial system set up and testing;
- * Upon agreement and request, provide ongoing support to the E-Mall Operations Administrator as contracted and/or on a time and materials basis.

Relevant Documents and Agreements

- * Agrees to abide by the **Operating Rules**.
- * Signs contract and agrees to Task Order with Policy Authority for provision of services and related products.

E. Technical Requirements

For this pilot, the State User Department agrees to comply with the technical standards which are detailed below:

E.1. User Personal Computer:

The minimum computer requirements and configuration is detailed below:

E.1.1. Internet and World Wide Web Connectivity

A computer capable of accessing the World Wide Web (WWW), which implies connectivity to the Internet using the TCP/IP protocol.

E.1.2. Hardware:

- Pentium Processor
- 32MB memory
- 10 MB of available disk space on the hard drive
- 10/100 Ethernet network interface card

- A mouse
- Year 2000 compliant
- Monitor: 17 inch or greater SVGA monitor, with a minimum of 800X600 pixels of resolution
- ADA compliant

E.1.3. Software:

- Windows 95 or Windows NT 4.0 Workstation
- A 4.0 or higher version of the Netscape Navigator or Internet Explorer browser to allow the use of Secure Sockets Layer (SSL) 3.0
- A Public Key Certificate to be installed within the user's browser and used to authenticate the identity of a User will be issued by the Certificate Manufacturer contracted to provide services to the E-Mall
- Year 2000 compliant.
- ADA compliant

Comparable hardware and software is acceptable but resolution of problems arising from their use is the sole responsibility of the user department.

E.2. Supplier Partner

Every party that agrees to perform the role of a Supplier Partner must, at a minimum, provide a web-based catalog that is compliant with the OBI 1.1 specification, as referenced under these Operating Rules.

E.3. Physical Security of Computing and Network Resources

The E-Mall Web Server must be kept in a physically secure location such that unauthorized persons can not gain physical access to the server without breaking and entering. There are no physical security requirements for Users during the course of the pilot, however, no User may permit an unauthorized person to gain access to a computer that is currently accessing a restricted area of the E-Mall server (that is, once a user logs onto the system with a username, password and Certificate, that user should not leave their computer accessible to any other person until logging off the E-Mall server). There are no physical security requirements for Suppliers during the course of the pilot. The Certificate Manufacturer must assure that no unauthorized personnel may gain physical access to the private key for the root Certificate for this pilot or may otherwise become capable of manufacturing unauthorized Certificates.

F. Duties and Obligations of the Parties

F.1. Electronic Offer and Acceptance

The terms ***OBI Order Request*** and ***OBI Order*** are to be construed in accordance with the OBI 1.1 specification, as referenced in these Operating Rules. For purposes of this section, the term ***E-Mall Server*** shall mean the web server hosted on behalf of the State Partners for the purpose of conducting OBI-compliant transactions. For purposes of this section, the term ***Supplier Server*** shall mean the web server of a Supplier Partner for the purpose of conducting OBI-compliant transactions.

F.1.1. OBI Order Request

An OBI Order Request shall constitute a contractual offer by the Supplier Partner to sell the specified commodities at the specified price and other included terms once it has been successfully posted by the Shopper's web browser to the E-Mall Server at the agreed upon post-back URL.

F.1.2. OBI Order

An OBI Order shall constitute a contractual acceptance by the State Partner once it has been successfully posted by the E-Mall Server to the Supplier Server at the agreed upon post-back URL.

F.2. Notice

Every party that has been approved as a participant after having signed and delivered a participation agreement for the E-Mall Pilot is entitled to notice of any proposed amendment to these Operating Rules at least 14 calendar days prior to said amendments taking effect, unless otherwise agreed by all the parties. In the case of a State Partner, the person(s) who sign the State MOU and each authorized State Coordinator are entitled to receive notice and may be requested or required to pass along such notice to each subordinate user within their state if appropriate.

F.3. Participation Agreements

As noted under these Operating Rules, a party that performs an authorized role within the E-Mall must sign an agreement, known generally as a Participation Agreement. A key function of each Participation Agreement is to signify the assent of each party to abide by these Operating Rules. Parties who will assume a role within the E-Mall Pilot may retrieve a current version of their respective agreements in PDF form from the official E-

Mall web site. These agreements must be completed, signed, and returned to the E-Mall Business Administrator in order for any person to become an authorized E-Mall participant.

F.4. Confidentiality

Unless otherwise specified in these Operating Rules and related agreements and to the extent permitted under applicable law, all personally identifiable information related to the E-Mall pilot, including User information, usage statistics related to an individual user, the names of administrators, any telephone, address or other individually identifiable data should be considered confidential and should not be disclosed to any person outside of the E-Mall pilot. Similarly, no Pilot Participant should make any public statements including press releases, information available on a web site and slide presentation related to the E-Mall pilot or about any other person or organization's participation in the E-Mall pilot, unless that statement has first:

- * appeared on the official E-Mall web site, or
- * appeared in the public press, or
- * been approved by an E-Mall Administrator

F.5. Intellectual Property

These Operating Rules are subject to Copyright by the Commonwealth of Massachusetts in its capacity as sponsor of the Multi-State E-Mall. All rights reserved. Permission to reproduce this document is hereby granted provided that the following limitations on this right are observed: (1) all copies must clearly indicate that this work is published by and attributed to the Commonwealth of Massachusetts in its capacity as sponsor of the Multi-State E-Mall; and (2) all copies must include this notice of copyright.

"Multi-State E-Mall" is a trademark of the Commonwealth of Massachusetts in its capacity as sponsor of the Multi-State E-Mall.

