

# FEDERAL RESERVE BANKS' PASSWORD PRACTICE STATEMENT (PPS)

## INTRODUCTION

The Federal Reserve Banks (“FRBs”) will issue user IDs, passwords, passphrases and PINs (collectively referred to as “Password(s)”) to non-employees and other individuals to make use of certain FRB electronic access methods, in order to transact or access certain Federal Reserve Financial Services or other FRB business applications (collectively referred to as “FRB Business Applications”). This Password Practice Statement (“PPS”) describes the policies and practices of the FRBs, with respect to FRB-issued Passwords used to access FRB Business Applications, and sets forth the obligations of an external user of FRB-issued Passwords. An institution, otherwise known as a “Participant,” is a depository institution or other authorized entity that is subject to the provisions set forth in the Federal Reserve Banks’ Operating Circular 5, Electronic Access (“OC 5”), and the Certification Practice Statement (“CPS”), where applicable. This PPS sets forth certain security procedures and guidelines as referenced in OC 5 and Passwords are “Access Control Features” under OC 5. For purposes of this PPS, a subscriber (“Subscriber”) is a named individual employee or agent of a Participant who is issued Passwords to access FRB Business Applications. By accessing certain FRB Business Applications, by means of Passwords, the Participant and Subscriber agree to comply with the provisions of this PPS. An FRB Business Application may have other security requirements for access in addition to the use of Passwords; nothing in this PPS shall be construed to affect any such additional security requirement.

## PARTICIPANT & EUAC OBLIGATIONS

The Participant has overall responsibility for and is liable, as described in OC 5, for all Passwords issued to the Participant’s Subscribers by the FRBs. Specifically, the Participant has the following responsibilities and obligations:

1. The Participant must identify the names and contact information for at least two (2) Participant security contacts, generally known as End User Authorization Contacts (“EUAC(s)”).<sup>1</sup> The identification must be provided to the FRBs in a writing signed and dated by an authorized Participant representative. The Participant is also responsible for informing the FRBs, in accordance with the FRBs’ then current standard procedures, of all updates or changes made with respect to the EUAC.
2. The Participant must complete the necessary Subscriber information to request Passwords for the Subscriber.
3. The EUACs are solely responsible for the identification, authentication and notification processes between the Participant and the FRBs with respect to Subscribers. The Participant’s EUACs are responsible for keeping confidential all Passwords supplied to the EUACs. An EUAC shall only provide any applicable security information and/or

---

<sup>1</sup> EUAC is the term used for security contacts for all services accessed through FedLine<sup>®</sup> Web and FedLine Advantage<sup>SM</sup> electronic access methods. However, for Participants using the DOS-based FedLine access method, the person serving the role of security contact for the Participant will be the Local Security Administrator (“LSA”). The terms and conditions of this PPS applicable to EUACs also apply to LSAs and any other security contacts that are designated by their Participants to receive Password and related security information.

## FEDERAL RESERVE BANKS' PASSWORD PRACTICE STATEMENT (PPS)

Passwords to a Subscriber if the EUAC has first validated the identity of the Subscriber and has authorized the Subscriber to access an FRB Business Application. The EUAC must notify the FRBs immediately if Passwords should not be issued to the proposed Subscriber. The FRBs have no responsibility for, and may rely entirely upon, the EUAC to validate the identity and authority of that Participant's Subscribers, and the Subscribers' roles within the respective specified FRB Business Applications.

4. At least one of the Participant's EUACs must notify the FRBs prior to (or if impossible, immediately after) the occurrence of any of the following events:
  - (a) Subscriber's employment with the Participant is terminated;
  - (b) A Subscriber no longer requires or is authorized to have access to one or more FRB Business Application(s);
  - (c) The Subscriber knows or suspects that his or her Passwords have been disclosed to, or are known by, any other person or entity or the Passwords have, in some way, been compromised.

Any such notice automatically constitutes a Participant's request that the Subscriber's Passwords and access to affected FRB Business Applications be revoked.

The EUAC must notify the FRBs immediately following the occurrence of any of the following events:

1. The EUAC has not received Passwords from the FRBs within ten (10) business days of submitting the Subscriber request form;
2. The Subscriber has not received Passwords from the FRBs within ten (10) business days of the EUAC submitting the Subscriber request form;
3. The EUAC or Subscriber receives Passwords that display evidence of tampering; or
4. The Subscriber attempts to use the Passwords but is unable to access an authorized FRB Business Application.

The Participant is solely responsible for distributing the PPS to its Subscribers and for ensuring that the Participant's Subscribers comply with all of the provisions of this PPS, including but not limited to the "Subscriber Responsibilities," as detailed below.

**Once the FRBs have issued valid Passwords, thereby granting the Subscriber access to an FRB Business Application, any instructions sent thereafter within an FRB Business application that utilizes any of those Passwords, will bind the Participant as fully as if the instructions had been expressly authorized and sent by the Participant.** All notices provided hereunder must be sent to the FRBs in accordance with the FRBs' instructions.

### SUBSCRIBER RESPONSIBILITIES

Subscribers are responsible for complying with all of the provisions of this PPS, including but not limited to the following specific Subscriber obligations:

1. Subscribers must maintain the confidentiality of the Passwords.

## FEDERAL RESERVE BANKS' PASSWORD PRACTICE STATEMENT (PPS)

2. Subscribers must retain exclusive control of the Passwords. Subscribers must not divulge or share Passwords with any other person or entity.
3. Subscribers are responsible for selecting strong passwords and passphrases. The following practices are strongly recommended by the Federal Reserve Banks:
  - (a) Subscribers should use a combination of upper and lower case alpha characters (e.g. b,B), alphanumeric characters (e.g. 6, 11) and special characters (e.g. !, &);
  - (b) Subscribers should not use sequential or repetitive characters;
  - (c) Subscribers should not use their (or Family members') names, nicknames, or initials in any form (forwards or backwards);
  - (d) Subscribers should not use their user IDs (unique identifiers provided by the FRBs) in any form;
  - (e) Subscribers should not use information about themselves or family members that can be easily obtained (e.g. birth dates, telephone numbers, social security numbers, etc.);
  - (f) Subscribers should not use words that would appear in a dictionary – English or otherwise.
4. Subscribers must comply with OC 5, including the CPS and this PPS, as applicable, as well as all other applicable security procedures, including those distributed or posted on [www.frbservices.org](http://www.frbservices.org) pertaining to Passwords.
5. Subscribers must notify their Participant's EUAC if they have not received any Passwords that they expect to receive from the FRBs.
6. Subscribers must notify their Participant's EUAC if Subscribers know or suspect that their Passwords have been disclosed to, or are known by, any other person or entity or the Passwords have, in some way, been compromised.
7. Subscribers must notify their Participant's EUAC if Subscribers are unable to recall Passwords.
8. Subscribers must notify their Participant's EUAC if they are unable, through the use of the Passwords, to access the appropriate FRB Business Application.
9. Subscribers must utilize the Passwords solely in the manner for which they are intended, only to access FRB business applications that their Participant has authorized them to access.

The Financial Services logo, "FedLine Advantage" and "FedLine" are either registered or unregistered trademarks or service marks of the Federal Reserve Banks. A complete list of marks owned by the Federal Reserve Banks is available at [www.frbservices.org](http://www.frbservices.org).