External User Account Request Form
For the Electronic Project Management (ePM) System

INSTRUCTIONS:

1. Complete this form, making sure to type your LEGAL name in the box provided below the Rules of Behavior agreement.
2. **PRINT** the completed form and sign your legal signature in the box provided below the Rules of Behavior agreement.
3. **SCAN** the completed, signed form and save a copy of the form to your desktop in the following format: firstnamelastnameexternal.pdf (example: johnsmithexternal.pdf)
4. When you have completed steps 1-3, please **EMAIL** the form to the Regional Approving Authority.

User Contact Information

Date of Request:	*Business E-Mail Address:
*First Name:	*Business Phone:
*Middle Initial: *If you do not have a middle initial please indicate this by entering* NMN*.*	Alternate Business Phone:
*Last Name:	Business Fax:
*Title:	*Region:

(Note: Type or print your name as it appears on your interim or adjudicated clearance letter).
* Indicates required fields.

User Affiliation Details

*Agency or Company:	Company DUNS Number**:

**DUNS No. is only required if your company is private and NOT a Federal Agency.

Note: To receive an ePM account, you must have an interim or adjudicated clearance.

Regional Approving Authority:

Regional Authority Email Address

Type or print the name and email address of the Regional Approving Authority. If you are uncertain about who is your Regional Approving Authority, contact your Project Manager or the Regional System Administrator.

FOR ePM SYSTEM ADMINISTRATOR USE ONLY

Comments:

Date Received:

Rules of Behavior for External Users

All external ePM users are required to review and agree to Rules of Behavior before using ePM.

You must not change your assigned password until you are authorized to by an ePM System Administrator.

You must comply with copyright and site licenses of proprietary software.

You must process only data that pertains to official business and is authorized to be processed on the system.

You must discontinue use of any system resources that show signs of being infected by a virus and report the suspected virus.

You must use only the data for which they have been granted authorization.

Your level of access to the ePM system is limited to ensure your access is no more than necessary to perform your legitimate tasks or assigned duties. If you believe you are being granted access that you should not have, you must immediately notify the ePM Information System Security Officer or the GSA National Help Desk (866-450-5250).

You must challenge unauthorized personnel in their work area.

You must ensure that access to application-specific sensitive data is based on job function.

You must maintain the confidentiality of your authentication credentials such as your password. Do not reveal your authentication credentials to anyone; a GSA employee should never ask you to reveal them.

You must follow proper logon/logoff procedures. You must manually logon to your session; do not store you password locally on your system or utilize any automated logon capabilities. You must promptly logoff when session access is no longer needed. If a logoff function is unavailable, you must close your browser. Never leave your computer unattended while logged into the system.

You must report all security incidents or suspected incidents (e.g., lost passwords, improper or suspicious acts) related to the GSA system to the ePM Information System Security Officer or the GSA National Help Desk (866-450-5250).

You must not establish any unauthorized interfaces between GSA applications and other non-GSA systems.

Your access to the GSA system is governed by, and subject to, Federal law, including, but not limited to, the Privacy Act, 5 U.S.C. 552a, if the applicable GSA system maintains individual Privacy Act information. Your access to the GSA system constitutes your consent to the retrieval and disclosure of the information within the scope of your authorized access, subject to the Privacy Act, and applicable Federal laws.

You must ensure that Sensitive information sent to a fax or printer is handled in a secure manner, e.g., cover sheet to contain statement that information being faxed is Sensitive But Unclassified, For Official Use Only, etc.

You must safeguard system resources against waste, loss, abuse, unauthorized use or disclosure, and misappropriation.

You must not process classified national security information on the system.

You must not browse, search or reveal GSA system information except in accordance with that which is required to perform your legitimate tasks or assigned duties.

You must not retrieve information, or in any other way disclose information, for someone who does not have authority to access that information.

You must not reconfigure hardware or software on the ePM or its interfaces.

You must follow all GSA wireless access policies.

You must ensure that Sensitive information is protected against unauthorized access by encryption according to GSA standards when sending via electronic means (telecommunications networks, e-mail, and/or facsimile).

You must ensure that Web browsers use Secure Socket Layer (SSL) version 3.0 (or higher) and Transport Layer Security (TLS) 1.0 (or higher). SSL and TLS must use a minimum of 256-bit, encryption.

You must ensure that Web browsers warn about invalid site certificates.

You must ensure that Web browsers warn if the user is changing between secure and non-secure mode.

You must ensure that your ePM Web browser window is closed before navigating to other sites/domains.

You must ensure that Web browsers check for a publisher's certificate revocation.

You must ensure that Web browsers check for server certificate revocation.

You must ensure that Web browsers check for signatures on downloaded files.

You must ensure that Web browsers empty/delete temporary Internet files when the browser is closed.

You must ensure that Web browsers warn if forms submittal is being redirected.

You must ensure that Web browsers do not allow access to data sources across domains.

You must ensure that Web browsers do not allow the navigation of sub-frames across different domains.

You must ensure that Web browsers do not allow the submission of non-encrypted form data.

There is a formal sanctions process with possible civil or criminal penalties for violations of the ePM Rules of Behavior.

You must agree to abide by the requirements set forth in GSA Order 3490.1A. (Please ask your Approving Authority for a copy of this document if it has not been provided to you.)

By your signature you must agree to these rules.

You should contact your ePM Information System Security Officer or the GSA National Help Desk (866-450-5250) if you do not understand any of these rules.

ACCEPTANCE
I have read the above Rules of Behavior for External Users of electronic Project Management (ePM). By my signature below, I acknowledge and agree that my access to ePM is covered by, and subject to, such Rules. Further, I acknowledge and accept that any violation by me of these Rules may subject me to civil and/or criminal actions and that ePM retains the right, at its sole discretion, to terminate, cancel or suspend my access rights to the ePM system at any time, without notice.

User's Legal Name: (Typed)

User's Signature: (Signature)

Date: