FedRAMP Package Access Request Form

For Review of a FedRAMP Security Package

Version 6.0

INSTRUCTIONS:

1. Please complete this form, then digitally sign.
2. Distribute to your FedRAMP approver for review and signature.
3. Please email your signed request form to info@fedramp.gov.

You must have a .gov or .mil email address to access a FedRAMP Security Package

NOTE: By signing this form, you agree to the rules of behavior described in the below sections. Agency personnel may work directly with cloud service providers (CSPs) to gain additional privileges to their documentation.

User Information

Date of Request:		**Agency or Department:**	
First Name:		**Bureau:**	
Last Name:		**Office:**	
E-Mail Address:		**Phone:**	

Select one: ◯ Federal Employee

◯ Federal Contractor – If yes, what company? _____

***If you are a federal contractor**, please also review Attachment A: Federal Contractor Non Disclosure Agreement for FedRAMP, sign, and attach to this request.*

Requested Package

Name of Package Requested: _____

What is the Package ID (located on the CSP listing on marketplace.fedramp.gov)?

_____

If you are not a current customer and an Authority to Operate (ATO) letter has not been provided to the FedRAMP PMO, access is granted for 60 days in order to properly ensure a high level of access control and maintain proper security over the security authorization packages. Permanent access is only granted to CSP customers who have provided the FedRAMP PMO with an ATO letter for the cloud service offering (CSO) in use.

Access Authorization

All reviewers are required to use multi-factor authentication via PIV (Personal Identity Verification) card to obtain access to the FedRAMP secure repository on the MAX.Gov. Please go to https://www.max.gov to register.

In order to gain access to the FedRAMP secure repository, the FedRAMP PMO requires approval from an authorized FedRAMP approver. This is your agency CIO, CISO, or someone they have designated.

Authorized FedRAMP Approver:

First Name:		**Title:**	
Last Name:		**Agency or Department:**	
Phone:		**Bureau:**	
E-Mail Address:		**Office:**	

Agreement for Package Reviewers

Instructions: Please initial each box

By completing and submitting this form you have confirmed and agree to the following:

	I agree to abide by all security and record management policies, standards, and procedures of my respective agency. I also agree to abide by the General Rules of Behavior outlined in this Agreement. If my agency's security and record management policies conflict with these General Rules of Behavior, I will consult with the FedRAMP PMO prior to accessing any of the documents provided by the FedRAMP PMO.
	I understand that GSA may monitor and audit my usage of my account and that using the system constitutes consent to such monitoring.
	I agree to use FedRAMP packages only for authorized purposes related to official business.
	I have a .gov or .mil email account that is registered on https://www.max.gov.
	I will not disclose information in FedRAMP Security Packages to any third-parties (i.e., any parties not expressly authorized to have access to the information by the FedRAMP PMO or the company that submitted the security package).
	I will not save, print, email, post, publish, or reproduce any FedRAMP Security Package documents in any form including all electronic methods, except to the extent necessary for internal evaluation of the FedRAMP Security Package as part of the agency authorization activities. Any documents that are saved, emailed, posted, published, or reproduced will be stored only on authorized U.S. Government systems and in the manner required to protect controlled unclassified information (CUI).
	Once my review is complete, I agree to destroy and delete all copies of the FedRAMP Security Package documentation provided under this Agreement.

	I agree to store FedRAMP Security Package documentation only on government furnished equipment and devices and subject to the same standards as my agency and the FedRAMP PMO General Rules of Behavior. I will not store FedRAMP Security Package documents on non-government equipment and devices.
	The undersigned prospective package reviewer certifies that the information listed above is current and accurate.
	I'm requesting access for the purposes of granting a security authorization for the cloud service referenced in this request, as well as for ongoing monitoring of the cloud service provider's security implementation.
	I understand and acknowledge that violation of this agreement is subject to the federal criminal prohibitions on theft of proprietary information and trade secrets by government employees, 18 U.S.C. § 1905, and theft of trade secrets for commercial advantage, 18 U.S.C. § 1832, which makes it a crime to take or use without authorization such information and to attempt or conspire to engage in such misconduct. The company that submitted the security package is a cloud service provider to GSA under FedRAMP. I acknowledge that (i) any FedRAMP Security Package documents and any other confidential information disclosed to Recipient under this Agreement are the proprietary technical or commercial information or trade secret information of the submitting company and (ii) the submitting company is an intended third-party beneficiary of this Agreement and may enforce its terms with respect to such information directly through an action in any court of competent jurisdiction.

User's Signature: _____ Date: _____

Agreement for Authorized FedRAMP Approver

If the user, which I am certifying, leaves my agency for any reason, or transfers to a different department, I agree to notify info@fedramp.gov of their departure from my supervision immediately.

Instructions: Please initial each box

	I am a federal employee.
	I have the authority to grant FISMA authorizations for my agency, or have been delegated by such authority to approve FedRAMP Package Access Request Forms on behalf of my agency.
	The person requesting access to the security package is acting requesting access for official government purposes.
	I agree to ensure that the package reviewer acts, in accordance with, the rules of behavior cited and agreed to.
	When the package reviewer no longer needs access, I will notify the FedRAMP PMO.

The undersigned authorized FedRAMP approver certifies that the information listed above is current and accurate.

Authorized FedRAMP Approver (please print): _____

Authorized FedRAMP Approver's Signature: _____ Date: _____

Attachment A: Federal Contractor Non Disclosure Agreement for FedRAMP

THIS NONDISCLOSURE AGREEMENT is entered into as of the date signed below by GSA, which is the party disclosing confidential information, and _____, who is the party receiving confidential information ("Recipient"), in order to protect the confidential information which is disclosed to Recipient by GSA.

NOW THEREFORE, in consideration of the mutual covenants contained herein, the parties hereto agree as follows:

1. This Non-Disclosure Agreement ("Agreement") is supplemental to the FedRAMP Package Access Request Form For Review of FedRAMP Security Package ("Access Request Form") to which Recipient has agreed. In the event of a conflict between this Agreement and the Access Request Form, the Access Request Form shall control.
2. The Confidential Information disclosed by GSA under this Agreement is: confidential and proprietary security authorization materials for the Federal Risk and Authorization Management Program (FedRAMP).
3. The Recipient shall keep the confidential information confidential and shall use the Confidential Information only for evaluation of a cloud service provider's security risk level in granting federal agency specific security authorizations and for ongoing monitoring of the cloud service provider's security implementation.
4. The Recipient shall not make any copies (electronic or otherwise) of the confidential information except as authorized in writing by the CSP. Any copied security package documentation should be stored consistently with the requirements for marking and storage of Controlled Unclassified Information ("CUI").
5. Recipient shall safeguard all Confidential Information (whether disclosed orally or otherwise) with at least the same degree of care (but no less than reasonable care) as it uses to safeguard its own Confidential Information of like kind. Recipient shall limit distribution of Confidential Information that it receives pursuant to this Agreement to its employees who have a need to know the information for the purposes set forth in Paragraph 3 and who have previously agreed to be bound by confidentiality obligations no less stringent than those in this Agreement and the online Agreement for Package Reviewers to which Recipient has agreed.
6. This agreement controls only confidential information which is disclosed to Recipient between the effective date (the date of last signature) and the end of the cloud service provider's authority to operate as defined in the ATO letter.
7. Recipient's duties under Paragraphs 3, 4 and 5 of this Agreement shall expire twenty (20) years after the expiration of the cloud service provider's authority to operate as defined in the ATO letter. Upon written request by GSA on or before the expiration of the confidentiality period as set forth herein, Recipient shall certify that it has no Confidential Information in its possession and that it has destroyed or deleted all Confidential Information that has been disclosed to it in electronic format.
8. This Agreement imposes no obligation upon the Recipient with respect to confidential information which (a) was in the Recipient's possession before receipt from FedRAMP; (b) is or becomes a matter of public knowledge through no fault of the Recipient; (c) is received by the Recipient from a third party without a duty of confidentiality; (d) is independently disclosed by the Recipient with GSA's prior written approval, or (e) is developed by the Recipient without reference to information disclosed hereunder.

9. FedRAMP warrants that it has the right to make the disclosures under this Agreement.
10. Neither party acquires any intellectual property rights under this Agreement.
11. I am aware that an unauthorized disclosure of any proprietary or confidential information or CUI may subject me to breach of contract claims as well as criminal, civil, and/or administrative penalties.
12. Appropriations Act restriction: These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958; section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b)(8) of title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive order and listed statutes are incorporated into this agreement and are controlling.
13. The parties do not intend that any agency or partnership relationship be created between them by this Agreement. With respect to any confidential information disclosed to Recipient under this Agreement that is the proprietary technical or commercial information or trade secret information of a cloud service provider to GSA under FedRAMP, such cloud service provider is an intended third-party beneficiary of this Agreement and may enforce its terms with respect to such information directly through an action in any court of competent jurisdiction.
14. All additions or modifications to this Agreement must be in writing and signed by both parties.
15. This Agreement is made under and shall be governed by the laws of the United States.
16. This Agreement may be terminated immediately by either party upon delivery of written notice of termination to the other party. Such termination shall not affect Recipient's duties with respect to confidential information disclosed prior to termination including without limitation those under Section 7, above.

SIGNED

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date of the last signature below

Federal Contractor Name (please print): _____

Federal Contractor Signature: _____ Date: _____