# FedRAMP Standard Contract Language

FedRAMP has developed a security contract clause template to assist federal agencies in procuring cloud-based services. This template should be reviewed by a Federal agency's Office of General Counsel (OGC) to ensure it meets all agency requirements, and then incorporated into the security assessment section of a solicitation. The clauses cover FedRAMP requirements for areas like the security assessment process and related ongoing assessment and authorization. The template also provides basic security requirements identifying Cloud Service Provider responsibilities for privacy and security, protection of government data, personnel background screening and security deliverables with associated frequencies.

The FedRAMP process discretely identifies some security control implementations as either the consumer's responsibility to implement or as a shared responsibility between provider and consumer. Consumer responsibility controls are incumbent upon the agency to implement and agencies are advised to consider security responsibilities in their program planning. Federal agencies must still make a risk-based decision about the applicability of storing and using Federal data in an information system. Ultimately, the security clauses are templates; they should be reviewed against mission requirements and tailored if agency policy warrants modification.

---

## Compliance Section

### FedRAMP Information Technology Systems Security Requirements:

In his December 8, 2011 memo titled "Security Authorization of Information Systems in Cloud Computing Environments," the Federal CIO established policy for the protection of Federal information in cloud services under the Federal Risk and Authorization Management Program (FedRAMP). Under the FedRAMP policy, agencies with leveraging existing cloud based -services or acquiring cloud based services (other than private cloud-based services) must initiate an authorization and use the FedRAMP information security and privacy requirements (including security and privacy controls, and controls selected for continuous monitoring) for cloud services to support authorization decisions.

Agencies can leverage cloud services assessed and granted provisional authorization through the FedRAMP process to increase efficiency and ensuring security compliance. The following security requirements apply to the services provided in the (contact/task order description).

The Federal agency will determine the security category for the cloud system in accordance with Federal Information Processing Standard 199; then, the contractor[1] shall apply the appropriate set of impact baseline controls as required in the FedRAMP Cloud Computing Security Requirements Baseline document to ensure compliance to security standards. The FedRAMP baseline controls are based on NIST Special Publication 800-53, Revision 3, Recommended Security Controls for Federal Information

[1] Contractor shall refer to cloud service providers, or contract holders who are providing cloud computing services to the Federal Government through this contract.

Systems and Organizations (as amended), and also includes a set of additional controls for use within systems providing cloud services to the federal government.

The contractor shall maintain a security management continuous monitoring environment that meets or exceeds the requirements in the Reporting and Continuous Monitoring (section xxx of this contract/Task Order) based upon the latest edition of FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements.

## *Additional Text for cloud services implemented or acquired before operation of FedRAMP:

*For all currently implemented cloud services and those services currently in the acquisition process prior to June 5, 2012, Federal agencies are required to submit an authorization package to the FedRAMP PMO (or have the contractor prepare the authorization package and submit the package to the FedRAMP PMO) upon completion. All cloud services currently implemented or those in the acquisition process prior to June 5, 2012 must meet all FedRAMP requirements by June 5, 2014.

## FedRAMP Privacy Requirements:

Contractor shall be responsible for the following privacy and security safeguards:

1. To the extent required to carry out the FedRAMP assessment and authorization process and FedRAMP continuous monitoring, to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the Contractor, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.
2. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.
3. The contractor shall also comply with any additional FedRAMP privacy requirements.
4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. In accordance with the Federal Acquisitions Regulations (FAR) clause 52.239-1, contractor shall be responsible for the following privacy and security safeguards:

    (a)The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. *Exception - Disclosure to a Consumer Agency for purposes of C&A verification.*

    (b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases

within XX hours. (FedRAMP recommends 72 hours) The program of inspection shall include, but is not limited to:

- Authenticated and unauthenticated operating system/network vulnerability scans
- Authenticated and unauthenticated web application vulnerability scans
- Authenticated and unauthenticated database application vulnerability scans
- Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools.

(c) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

If the vendor chooses to run its own automated scans or audits, results from these scans may, at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided, in full, to the Government.

**SENSITIVE INFORMATION STORAGE**

Sensitive But Unclassified (SBU) information, data, and/or equipment will only be disclosed to authorized personnel on a Need-To-Know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST Special Publication 800-88, *Guidelines for Media Sanitization*.

The disposition of all data will be at the written direction of the COR, this may include documents returned to Government control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

**PROTECTION OF INFORMATION**

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. The contractor shall also protect all Government data, equipment, etc. by treating the information as sensitive. All information about the systems gathered or created under this contract should be considered as SBU information. It is anticipated that this information will be gathered, created, and stored within the primary work location. If contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

The government will retain unrestricted rights to government data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

The data that is processed and stored by the various applications within the network infrastructure contains financial data as well as personally identifiable information (PII). This data and PII shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The contractor shall ensure that the facilities that house the network infrastructure are physically secure.

The data must be available to the Government upon request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

No data shall be released by the Contractor without the consent of the Government in writing. All requests for release must be submitted in writing to the COR/CO.

**SECURITY CLASSIFICATION**

The preparation of the deliverables in this contract will be completed at a Sensitive but Unclassified level.

**CONFIDENTIALITY AND NONDISCLOSURE**

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the contractor in the performance of this contract, are the property of the U.S. Government and must be submitted to the COTR at the conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials in accordance with FAR 52.227-14.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced, or retained by the contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The contractor shall not release any information without the written consent of the Contracting Officer.

Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

Additionally,

**Disclosure of Information**

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of

the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

# Security Requirements Section

## FedRAMP Security Requirements Overview:

The minimum requirements for low and moderate impact cloud systems are contained within the FedRAMP Cloud Computing Security Requirements Baseline. The contractor and Federal Government Agency share responsibility to ensure compliance with security requirements.

The implementation of a new Federal Government cloud system requires a formal process, known as Assessment and Authorization, which provides guidelines for performing the assessment.

FedRAMP requires cloud service providers to utilize a Third-Party Assessment Organization (3PAO) to perform an assessment of the cloud service provider's security controls to determine the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting security requirements.[2]

The FedRAMP PMO security staff will be available for consultation during the process. Both the FedRAMP PMO staff and JAB will review the results before issuing a Provisional Authorization decision. The Government reserves the right to verify the infrastructure and security test results before issuing an Authorization decision.

Federal agencies will be able to leverage the provisional Authorization granted by FedRAMP and any documentation prepared by the contractor to issue their own authority to operate.

The vendor is advised to review the FedRAMP guidance documents (see References below) to determine the level of effort that will be necessary to complete the requirements. All FedRAMP documents and templates are available at http://FedRAMP.gov.

## FedRAMP Security Compliance Requirements:

The contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for low and moderate impact system (as defined in FIPS 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for both low and moderate impact systems. While the FedRAMP baseline controls are based on NIST Special Publication 800-53, Revision 3.

[2] The FedRAMP JAB will not review authorization packages assembled by non-accredited third-party assessors. Contractors can find the list of FedRAMP-accredited 3PAOs at www.FedRAMP.gov.

The contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

## Required FedRAMP Policies and Regulations:

OMB Memo Security Authorization of Information Systems in Cloud Computing Environments

## Assessment and Authorization

(Agency) may choose to cancel the (Contract/award) and terminate any outstanding orders if the contractor has its provisional authorization revoked and the deficiencies are greater than agency risk tolerance thresholds.

## Assessment of the System:

1. The contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. The contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at http://FedRAMP.gov :
    - Privacy Impact Assessment (PIA)
    - FedRAMP Test Procedures and Results
    - Security Assessment Report (SAR)
    - System Security Plan (SSP)
    - IT System Contingency Plan (CP)
    - IT System Contingency Plan (CP) Test Results
    - Plan of Action and Milestones (POA&M)
    - Continuous Monitoring Plan (CMP)
    - FedRAMP Control Tailoring Workbook
    - Control Implementation Summary Table
    - Results of Penetration Testing
    - Software Code Review
    - Interconnection Agreements/Service Level Agreements/Memorandum of Agreements
2. Information systems must be assessed by an accredited 3PAO whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.
3. The Government reserves the right to perform Penetration Testing. If the Government exercises this right, the contractor shall allow Government employees (or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with FedRAMP requirements. Review activities include but are not limited to scanning operating systems , web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support

structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

4. Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the contractor's implementation as documented in the Security Assessment Report shall be tracked by the contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the gaps, the Government may require them to be remediated before a provisional authorization is issued.
5. The contractor is responsible for mitigating all security risks found during A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 30 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

## Authorization of System:

The contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. The Government reserves the right to conduct on site inspections. The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.

## Reporting and Continuous Monitoring:

Maintenance of the FedRAMP Provisional Authorization will be through continuous monitoring and periodic audit of the operational controls within a contractor's system, environment, and processes to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to the FedRAMP PMO as required by FedRAMP Requirements. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the FedRAMP JAB to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors will be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

**Additional Stipulations:**

1. The FedRAMP deliverables shall be labeled "CONTROLLED UNCLASSIFIED INFORMATION" (CUI) or contractor selected designation per document sensitivity. External transmission/dissemination of FOUO and CUI to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, "Security requirements for Cryptographic Modules."
2. Federal Desktop Core Configuration & US Government Configuration Baseline: The contractor shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC) and US Government Configuration Baseline (USGCB). The standard installation, operation, maintenance, updates, and/or patching of

software shall not alter the configuration settings from the approved FDCC/USGCB configuration. Offerings that require installation should follow OMB memorandum 07-18. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use Security Content Automation Protocol (SCAP) validated tools with FDCC/USGCB Scanner capability to certify their products operate correctly with FDCC/USGCB configurations and do not alter FDCC/USGCB settings.

3. As prescribed in the Federal Acquisition Regulation (FAR) Part 24.104, if the system involves the design, development, or operation of a system of records on individuals, the contractor shall implement requirements in FAR clause 52.224-1, "Privacy Act Notification" and FAR clause 52.224-2, "Privacy Act."
4. The contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.

## References:

- FedRAMP Cloud Computing Security Requirements Baseline http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_Final.zip
- FedRAMP Concept of Operations http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_Final.zip
- FedRAMP Templates http://www.gsa.gov/graphics/staffoffices/Updated_Templates_Final.zip