

COALFIRE FASTRAMP 360 SERVICES DESCRIPTION

This Service Description describes Coalfire's FastRAMP 360. All capitalized terms in this Service Description have the meaning defined in the Agreement or relevant Service Order under which the Service was purchased. This Service Description, with any attachments included by reference, is part of and incorporated into Client's manually or digitally-signed agreement with Coalfire which reasonably governs the use of the Service, or if no signed agreement exists, the Service Agreement found at: <https://www.coalfire.com/agreements/sa> (together, the "Agreement").

Summary: Coalfire's FastRAMP 360 Service ("Services") will assist Client with: (a) assessing and building an environment that meets the controls mandated by the Federal Risk and Authorization Management Program ("FedRAMP"); (b) monitoring Client's environment for risks associated with non-compliance of FedRAMP controls; and (c) managing Client's environment in order to stay compliant with FedRAMP controls.

TABLE OF CONTENTS

1. Services Overview

- A. Dedicated Personnel and Communication Cadence
 - A-1 Client Point of Contact
 - A-2 Meetings
 - A-3 Executive Report
- B. Alignment and Confirmation Services
 - B-1 Technical Specifications
 - B-2 Workload Architecture and Authorization Boundary
 - B-3 Management Architecture and Reference Architecture Design Document
 - B-4 Workload Gap Analysis Workbook
- C. Onboarding Services
 - C-1 FedRAMP Security Systems Plan and Policies, Plans & Supporting Documentation Development
 - C-2 Deployment Capabilities and Implementation / Operational Responsibilities
 - C-3 FedRAMP Initial Authorization Documentation Index
 - C-4 Onboarding Validation Services
- D. Steady-State Operation Services
 - D-1 Audit & Compliance Management
 - D-2 Availability & Continuity Management
 - D-3 Continuous Monitoring & Vulnerability Management
 - D-4 Event Monitoring & Incident Management
 - D-5 Change Management
 - D-6 Patch Management
 - D-7 Access Management
 - D-8 Reports and Documents

2. Additional Terms and Conditions

- A. Regulatory Changes
- B. Third Party Applications
- C. Disclaimer of Liability
- D. Use of Coalfire Equipment
- E. Coalfire Affiliates / Subcontractors

1. SERVICE OVERVIEW

A. Dedicated Personnel and Communications Cadence. The Service includes a Customer Success Manager (“CSM”) dedicated to Client during the term of the Service. The CSM is responsible for understanding the Client’s core business needs to facilitate mutually agreed upon outcomes. In addition to serving as an advocate on behalf of the Client and acting as an escalation point, CSMs can assist with the following:

- Scheduling the Services Kickoff meeting
- Facilitation of Onboarding and on-going activities
- Clarification on the scope of Service
- Change Order process
- Access to a solution to support document storage and transfer
- Communication of Services status and other applicable notifications
- Collecting Client communication and feedback
- Reviewing that all defined metrics are being met during operations
- Tracking, reporting and escalation of material risks and issues
- Recurring meetings with stakeholder team

A-1 Client Point of Contact. Client will designate one (1) employee to serve as a primary point of contact (“Client POC”) for the Service. The Client POC will be responsible for directly interfacing with the Coalfire CSM, as well as scheduling Client personnel for required meetings, interviews, and information collection to complete the Services.

A-2 Meetings. Coalfire and Client shall meet at the frequency and addressing the topics identified below.

- i. **Configuration Control Board Meeting.** A weekly meeting with Coalfire and Client stakeholders to discuss and consider proposed changes to Client’s environment, including workload code, infrastructure, patch management, upgrades, and other alterations.
- ii. **Continuous Monitoring Meeting.** A bi-weekly meeting with Coalfire and Client stakeholders to discuss vulnerability scan process, status, findings, deviation requests, remediation strategies and Plan of Action & Milestone (“POA&M”) updates.
- iii. **Continuous Monitoring Meeting (Sponsor/Federal PMO).** A monthly meeting with Coalfire, Client stakeholders and sponsor and/or Federal PMO stakeholder to reflect monthly updates to the vulnerability scan findings, deviation requests and POA&M updates.
- iv. **Business Review Meeting.** A quarterly meeting among Coalfire leadership, Client stakeholders and the CSM.
- v. **Client POC Meeting.** A weekly meeting with Client and CSM to review escalations.

A-3. Executive Report. Coalfire shall provide the following report during the Services.

Name	Description	Cadence
Executive Report	Coalfire shall provide a report to Client with details regarding incidents, events, special services and escalations relevant to the Services that have occurred during the past thirty (30) days.	Monthly

B. Alignment and Confirmation Services.

B-1 Technical Specifications. Coalfire will meet with Client to share FedRAMP requirements and collect information about Client technical requirements needed to be in place to properly install the workload within the designed environment (“Technical Specifications”). Coalfire will review this data to define the Client architecture’s eligibility for meeting the Services scope detailed in the relevant Service Order.

B-2 Workload Architecture and Authorization Boundary. Client will provide details of the Client workload code, and the Cloud Service Provider services upon which the Client workload code is deployed in order to run within the cloud (e.g., operating systems, containers, serverless functions, and databases) (“Workload Architecture”), and adequate detail of Client Technical Specifications. Coalfire and Client will mutually determine if any Workload Architecture changes are needed to meet FedRAMP requirements and define all components of an information system to be authorized for operation by the target authorizing compliance entity. This activity will define any excluded separately authorized systems to which the information system is connected (“Authorization Boundary”). Coalfire will present the Client with any additional findings from the Workload Gap Analysis which impact the system’s proposed Authorization Boundary and compliance, non-compliance, or partial compliance across all in-scope FedRAMP controls.

B-3 Management Architecture and Reference Architecture Design Document. Coalfire will develop a system design specific to the components that Coalfire will manage and provide management and security functions to support FedRAMP requirements (“Management Architecture”) and detail the integration of this boundary into the larger Workload Architecture (“Reference Architecture Design Document” or “RADD”). The RADD will be developed for the Client’s environment within the Authorization Boundary only. It will not include design details for environments outside of the Client’s environment, details related to development or workload process or procedures, or workload production runtime operations.

Name	Description
Executive Summary	(a) Services Overview and Scope, (b) Points of Contact, (c) System Overview, (d) Product Selection, (e) Design Considerations (Assumptions and Constraints, Client Dependencies)
Design Specifications	(a) Definition of Authorization Boundary in Scope, (b) Production Infrastructure Design Specifications (Production Infrastructure Design Specifications, Management Virtual Private Cloud (“VPC”) Infrastructure Overview, Routing between Management VPC and Workload VPCs, Dataflows, Network Segmentation for Security, Network Services, Compute Services, Storage Services, Database Services, Notification, Messaging, and Queue Services, Other / Miscellaneous Services) and (c) Management VPC Shared Services Specifications

B-4 Workload Gap Analysis Workbook. A review of the existing Client workload/information system to determine its compliance posture against requirements to include: identifying and verifying Authorization Boundary, conducting a technical review of controls implementation or plans, determining the sufficiency of security plans, policies, and procedures, and establishing a roadmap for authorization.

C. Onboarding Services. The final RADD will be used by Coalfire as the blueprint for these onboarding Services. Client's system infrastructure and tooling will be aligned to verify Client's logs, monitoring, and security tenets are in place in accordance with the Services scope detailed in the relevant Service Order. Each Party's responsibilities for the technical implementation for the cloud architecture will be performed according to the Implementation Responsibilities in the relevant Service Order. Client is responsible for providing a detailed list of test cases to be used during the Onboard Validation Services in Section D below. All defined compliance documentation will be generated in parallel with the architecture deployment, per Section D below.

Following the Alignment and Confirmation Services detailed in Section B above, and in parallel with this section, Coalfire will review Client's system infrastructure and tooling of the Management Architecture to confirm in-depth configuration alignment. This review may include, but are not limited to:

- Validation of configurations to meet the regulatory requirements detailed in the scope of Services in the relevant Service Order
- Tuning to confirms logs, monitoring, and security tenets are in place.
- Client-specific environment technical documentation created supporting continued operation of the tooling and infrastructure.

C-1 FedRAMP SSP and Policies, Plans, and Supporting Documentation Development. Coalfire will analyze the data during the information discovery session, as it relates to the in-scope FedRAMP controls, to understand the implementation status of each applicable security control before beginning documentation. The parties will align on a schedule at the beginning of this process. Coalfire will detail the Coalfire interaction of Management Architecture and activities related to applicable FedRAMP controls and documents and provided the written definitions ("FedRAMP ATO Documentation and Supporting Materials")

C-2 Deployment Capabilities and Implementation / Operational Responsibilities. The below table lists the categories of security tools commonly deployed during the Services. The specific tools and implementation responsibilities applicable to Client will be as defined in the applicable Service Order. Coalfire and Client shall share responsibilities of the design, implementation, and configuration of the cloud architecture, as detailed below, within the Authorization Boundary according to details in applicable Service Order.

Category	Capability
Management Plane Operating System(s)	Base cloud compute OS
Data Services	Data services for Management Plane
Vulnerability Management	Device and host-based Scanner
	Database scanner
	Web application scanner
	Configuration/compliance scanner
Configuration Management	Source Control Repositories
	Container Repositories
	Ticketing System
	Configuration and patch management
Network	Subnets and routing
	Load balancing
	Firewall rules

Category	Capability
	External Domain Name Services (DNS)
	Internal Domain Name Services (DNS)
Border Protection and VPN	Virtual Private Network (VPN)
Access Protections	Directory Services
	Multifactor Authentication (MFA)
Endpoint Protection	Anti-virus / malware
	File Integrity Monitoring (FIM)
	Host Intrusion Detection/Host Intrusion Prevention (HIPS/HIDS)
Monitoring and Logging	Security Information and Event Monitoring (SIEM)
Secrets Management	Secrets Management
	Key Management
	Certificate Authority
Communications and Notifications	Emails, paging alerts, and collaboration tools (as applicable)

C-3. FedRAMP Initial Authorization Documentation Index. The documentation identified below is a required part of the FedRAMP authorization package. Responsibilities for drafting and reviewing the documentation are listed in the table below.

Package Requirement	FedRAMP Template	Party to Draft	Party to Review
System Security Plan (“SSP”)	Yes	Coalfire	Client
SSP Attachment 1a – Information Security Policies (covering all control families)	No	Coalfire	Client
SSP Attachment 1b – Information Security Procedures (covering all control families)	No	Shared	Both
SSP Attachment 2 – User Guide	No	Client	N/A
SSP Attachment 3 – Digital Identity Worksheet	Included in Section 15 of the SSP template	Coalfire	Client
SSP Attachment 4 – Privacy Threshold Analysis	Included in Section 15 of the SSP template	Coalfire	Client
SSP Attachment 4 – Privacy Impact Assessment	Yes	Coalfire	Client
SSP Attachment 5 – Rules of Behavior	Yes	Coalfire	Client
SSP Attachment 6 – Information System Contingency Plan	Yes	Coalfire	Client
SSP Attachment 7 – Configuration Management Plan	No	Coalfire	Client
SSP Attachment 8 – Incident Response Plan	No	Coalfire	Client
SSP Attachment 9 – Control Implementation Summary Workbook	Yes	Coalfire	Client
SSP Attachment 10 – Federal Information Processing Standard 199	Included in Section 15 of the SSP template	Coalfire	Client
SSP Attachment 11 – Separation of Duties Matrix	No	Client	Coalfire

Package Requirement	FedRAMP Template	Party to Draft	Party to Review
SSP Attachment 12 – Laws and Regulations	Yes	N/A	N/A
SSP Attachment 13 – Integrated Inventory Workbook	Yes	Coalfire	Client

C-4 Onboarding Validation Services. Client will use the test cases identified during Onboarding Services in Section C above to validate applicable functionality.

D. Steady-State Operations Services. Coalfire will lead the following activities: development of procedures, audit evidence generation and collection, system operation, and maintenance of Client environments with a focus on performance in the areas defined below:

D-1 Audit & Compliance Management. Coalfire will support the initial and annual FedRAMP audits via interviews, documentation retrieval, and technical demonstrations of the system infrastructure and configuration. Coalfire will assist Client in Client's demonstrate of its ability to adherence to FedRAMP requirements by identifying Plan of Actions and Milestones action items for Client's mitigation and assist Client with Client's evidence collection demonstrating compliance with the in-scope security controls.

D-2 Availability & Continuity Management. Coalfire will assist with Client to handle availability and disaster recovery through load balancing, high-availability, or dynamic scalability through initial design and onboarding. The boundary can be hosted in multiple zones within the public cloud environment to meet availability requirements. Critical systems such as directory services and ingress methods (VPN) will be replicated in production. Storage replication will be achieved through using cloud native file-based storage services. Traffic failover for disaster recovery is achieved through cloud native DNS changes where possible. Backups of stacks are automated using cloud native persistent drives and associated native snapshots and can be restored in the event of a failure or outage to ensure business continuity. Workload and Management Architecture System-level, and User-level Data are backed up, in addition to the infrastructure, at scheduled intervals using automated processes.

In the event of a failure or outage that impacts Client's Workload and Management Architecture, or at the Client's request; Coalfire can perform a restore of any of the backups based on the details below.

i. **Virtual Server Disk Backups.** Coalfire will maintain at minimum four (4) concurrent daily backups of Virtual Server Disks in the form of snapshots. Virtual Server Disk snapshots will be retained for a minimum of four (4) days such that the oldest Virtual Server Disk snapshot is four (4) days prior to the current date.

ii. **Cloud Database Backups.** Coalfire will maintain at minimum seven (7) concurrent daily backups of Cloud Databases in the form of Cloud Database Backups. Cloud Database Backups will be retained for a minimum of seven (7) days such that the oldest Cloud Database Backup is seven (7) days prior to the current date.

iii. **Shared File System Backups.** Coalfire will maintain at minimum seven (7) concurrent daily backups of Shared Filesystems in the form of Shared File System Backups. Shared File System Backups will be retained for a minimum of seven (7) days such that the oldest Shared File System Backup is seven (7) days prior to the current date.

iv. **Disaster Recovery Testing.** Will assist with Disaster Recovery Testing once (1) annually.

D-3 Continuous Monitoring & Vulnerability Management. Coalfire will provide continuous monitoring of Client's security controls deployed in the Workload and Management Architecture and the evolving threats and changes to Client's environment. Coalfire will identify, prioritize, and remediate (within the Management Architecture) vulnerabilities through a structured lifecycle approach providing increased operational visibility and enabling a strong, repeatable process to identify vulnerability risk exposure. Each month, Coalfire will determine if the applicable systems and hosts are vulnerable to any security weakness as identified by the NIST National Vulnerability Database using the defined vulnerability scanning policy, procedures, and tools to help achieve and maintain security authorizations that meet FedRAMP requirements.

D-4 Event Monitoring & Incident Management. Coalfire provides 24x7x365 event monitoring and alerting and will respond to unplanned interruptions or reductions of quality of a service ("incidents") in accordance with the in table below. A full list of monitored events that includes criticality level and type of event, can be found within the Operations Playbook. Incidents will be managed within the Client ticketing system deployed within the compliance boundary. All incidents and changes will be tracked and ticketed within the system.

Criticality	Priority	Response Time**	Action Time***
Critical*	P1	30 minutes	1 hour
High	P2	4 hours	1 business day
Moderate	P3	1 business day	2 business days
Low	P4	3 business days	5 business days

*Except for Critical (P1), all times are based upon an 8am-5pm CST, Monday-Friday support schedule
 **"Response Time" is defined as the difference in time between the time the incident was created by the Client or system and the time Cloud Management Services (Section D) provides an initial response via email, ticketing system, phone call, or any other form.
 ***"Action Time" is the difference between incident creation and the start of remediation or restoration activities

D-5 Change Management. Coalfire is responsible for maintenance of Client's Workload and Management Architecture, which includes operating systems, databases, networking configurations, and supporting toolsets. Client will follow its own continuous integration / continuous delivery, which results in a complied binary or set of binaries. Coalfire is not responsible for maintenance activities or configuration issues aligned to the workload code binaries.

- Coalfire will utilize non-production (existing pre-production, staging, or other testing environment) to support the maintenance process, and functionally will mimic or enforce security tooling that exists in the production environment to better mirror that environment.
- The purpose of the non-production (pre-production, staging, or testing) environment is to verify that the workload is functional on the platform before production users can access the software.

Coalfire will support recurring Client workload code deployment at a mutually defined cadence within the confines of non-significant changes to the system boundary, to include the workload code itself.

Upon any new Workload and Management Architecture release or change, Coalfire will complete a Security Impact Analysis ("SIA"), defined within the Configuration Management Plan (see table in Section C-3; FedRAMP Initial Authorization Documentation Index), to determine any adverse security affects. Client will provide validation of any required underlying operational environment changes necessary to successfully deploy the new Workload and Management Architecture code. Deployment will be conducted at the direction of Coalfire and aligned with the cadence if the release is not deemed to be a Significant Change per compliance requirements, and if the SIA deems the change does not adversely affect the system or security functionality. Coalfire may invoke Downtime dependent upon the required changes and necessary processes. "Downtime" means all the time in a calendar month during which the production Application Plane or Management Plane infrastructure is not available.

D-6 Patch Management. The patch management process is enacted in the event a security or operational patch is identified through vulnerability scans, client request, or as part of a regular patching cadence ("Regular Maintenance Window"). In addition, when Workload and Management Architecture updates or patches are released by the respective vendor, they will be applied in a timely and consistent manner to minimize impact during Scheduled Downtime. "Scheduled Downtime means all of

the time of unavailability for the production of the Application Plane or Management Plane infrastructure that is scheduled by Coalfire.

In most cases, Coalfire will patch Workload and Management Architecture servers and instances during the Regular Maintenance Window, dependent on schedule and circumstances. Coalfire will endeavor to notify Client in real-time as to the progress of the emergency updates. The Regular Maintenance Window will be defined in the Operations Playbook listing cadence and timeframes. Coalfire reserves the right to extend or change the times of the Regular Maintenance Windows for Workload and Management Architecture cloud account(s), network(s), and infrastructure. Coalfire will use commercially reasonable efforts to notify Client at least 72 hours prior to the occurrence of a Scheduled Downtime for the production Workload Plane or Management Plane infrastructure.

D-7 Access Management. Coalfire will provision users with access to the Workload and Management Architecture and verify that the appropriate Access Management plans and policies are implemented and followed for that infrastructure once initial licensing and access for the Coalfire team has been established. The Client is responsible for defining and authorizing access requests, and Coalfire will be responsible for provisioning access to the Workload and Management Architecture and Client will provision access to the Workload Architecture.

Coalfire and the Client will have a shared responsibility for Access Management as Coalfire is considered a vendor from a compliance perspective and as such, the Client must approve all Coalfire personnel access to the Authorization Boundary and grant the appropriate rights. If Client wishes to maintain and manage access requests, Client is responsible for all facets of maintaining compliance documentation and corresponding evidence collection.

D-8 Reports and Documents. The following is a summary of the reports and documents to be provided by Coalfire under the Steady State Operations Services.

Name	Description	Cadence
Operations Playbook	Coalfire will develop and, if appropriate, update throughout the Services an Operations Playbook. Coalfire will evaluate Client's in-scope environment and identify FedRAMP operational processes and procedures that will assist Client to manage and run its infrastructure. The Operations Playbook may contain topics such as RACI tables, metrics, points of contact, service definitions, workflows, and other pertinent material.	Initial creation; Twice annual review
Procedures Document	Coalfire will develop the FedRAMP Procedures documents and detail specific implementations of Workload and Management Architecture controls within the following control families: Access Control, Audit and Accountability, Awareness and Training, Configuration Management, Contingency Planning, Identification and Authentication, Incident Response, Planning, Personnel Security, Risk Assessment, Security Assessment and Authorization, System and Communication Protection, System and Information Integrity, System and Services Acquisition.	One (1) Initial, two (2) Annual; audits held annually
Change Maintenance Report	Documented summary of the activities related to the vulnerability remediation process through workload of relevant patches, workarounds, or redeployments, as well as notation of configuration or architecture changes of the system and services within the Workload and Management Architecture.	Monthly
Patch Management Report	Documented summary of the activities related to the vulnerability remediation process through workload of relevant patches, workarounds, or redeployments, as well as notation of configuration or architecture changes of the system and services within the Workload and Management Architecture.	Monthly
Continuous Monitoring Report	This report will summarize incidents identified by Coalfire during the Continuous Monitoring Services, which may include topics such as: – Systems Inventory – Official Vulnerability Scans – Executive Summary – Plan of Actions and Milestones – Deviation Requests	Monthly
Cloud Deployment Supporting Documentation	Coalfire will assist Client in the creation of documentation related to Client's environment, toolsets, bootstrapping efforts, and other customizations utilized in cloud deployment and management. This documentation, and related deployment materials, are intended only for Client's environment only, expressly excluding design details for environments outside of the Client's environment, details related to development process or procedures, or production runtime operations. This documentation will be provided at the end of the engagement.	One-time

2. ADDITIONAL TERMS AND CONDITIONS.

A. Regulatory Changes. The Parties acknowledge that changes to compliance and/or security frameworks requirements that are implemented after the Effective Date of the relevant Service Order may affect how Coalfire performs the Services. If changes to those compliance and/or security frameworks requirements occur during the course of the Service, those changes will be addressed in a Change Order.

B. Third Party Applications. Pricing of the Services does not account for effort to support and/or change; (a) Client application changes required to meet compliance standards or; (b) cloud and Third Party vendor system changes needed for or resulting from Client application changes. Client is solely responsible for the procurement of and payment for services, solutions and/or licenses that are required to implement any third-party services within the deployed system ("Third Party Applications"). Prior to commencing Onboarding, Client will procure all required certificates and licenses for the Third Party Applications, as well as cloud infrastructure accounts. As a part of the RADD, Coalfire will provide a list of Third Party Applications that will be required to perform the Onboarding Services in Section C.

C. Disclaimer of Liability. Client acknowledges and agrees that Coalfire is not responsible for the any functionality or availability of any Third Party Applications, or for any underlying infrastructure environments within the deployed system, including, without limitation, any incompatibilities outside of Coalfire's control. Coalfire is not responsible for actions, omissions, or incidents outside of Coalfire's control, including, but not limited to: (i) Client's reliance upon third-party providers, including its cloud services provider, third party hardware/software providers, manufacturers and/or publishers, (ii) risks inherent in internet connectivity, and (iii) any actions or omissions by Client and its other third-party providers with regard to the environment.

D. Use of Coalfire Equipment. All Services may be performed on Coalfire equipment including but not limited to computers, laptops, storage locations, and portals.

E. Coalfire Affiliates/Subcontractors. Client will provide Coalfire and its affiliates or subcontractors providing the Services under this SOW continual full administrative level access, permissions, and any licenses required to access and use the Third Party Applications in connection with the Services, including in-boundary components connected to the environment, including local deployments both owned and licensed. Client will provide Coalfire ability and access to create, read, and update support tickets with Third Party Application vendors to troubleshoot and support workload operations.