Coalfire Compliance Essentials

Service Description

This Service Description describes Coalfire's Compliance Essentials ("Service"). All capitalized terms in this description have the meaning defined in the Agreement or in the Definitions section.

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 Terms and Conditions found at: https://www.coalfire.com/agreements/sa (together, the "Agreement").

Table of Contents

1: Technical/Business Functionality and Capabilities

Service Overview

The Compliance Essentials™ Service is a web-based assessment, risk, and compliance application designed to allow Clients to manage their data and evidence across multiple Information Security Framework Standards. During the Subscription Term, Client may use the Service in accordance with the Agreement.

Service Features

- Client can access the Service through a self-service online portal ("Portal"). Client may configure and manage the Service, and view dashboards, through the Portal.
- The Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis and is monitored for hardware availability, service capacity and network resource utilization. The Service is regularly monitored for service level compliance and adjustments are made as needed.
- The Service includes the following modules: Guided Compliance, Self-Assessment, Policy, Frameworks, and Scoping. Additional modules may be made available for an additional fee.
- Client may configure compliance Programs, add and assign users, upload, and manage documents and evidence, and perform assessments against supported Information Security Framework Standards, as currently enabled in the Portal.
- Client may upload, manage draft and publication status, and assign ownership of policy documentation through the Portal.
- Client may create and modify custom security frameworks through the Portal.

Add-On Services

The following add-on Services may be available. If purchased, this Service Description will apply to the delivery of the Add-On Services.

- Compliance Essentials Risk Management Add-On: This module enables both Client and Program level management of risk register, tracking, quantification, and treatment plans.
- Compliance Essentials Automation Add-On: This module enables the automatic collection and use of evidence from Client's systems. After configuring appropriate login credentials to provision Compliance Essentials read access to Client data sources, evidence will be periodically collected and used to help meet Client compliance needs inside of Compliance Essentials. Automation is metered by quantity of Programs with Automation, and quantity of Data Sources.

2: Client Responsibilities

Coalfire can only perform the Service if Client provides required information or performs required actions, otherwise performance of the Service may be delayed, impaired or prevented, and Client may lose eligibility for any Service Level Agreement.

- Setup Enablement: Client must provide information required for Coalfire to begin providing the Service.
- Adequate Client Personnel: Client must provide adequate personnel to assist Coalfire in delivery of the Service.

- Client must acquire and maintain all required licenses from third parties that are necessary for the enabled frameworks available in the Portal.
- Client Configurations vs. Default Settings: Client must configure the features of the Service through the Portal, if applicable, or default settings will apply. In some cases, default settings do not exist and no Service will be provided until Client chooses a setting. Configuration and use of the Service are entirely in Client's control, therefore, Client is not liable for Client's use of the Service, nor liable for any civil or criminal liability that may be incurred by Client as a result of the operation of the Service.

3: Entitlement and Subscription Information

Meter Metrics

The Service is available under the following Meter as specified in the Order Confirmation:

- "**Program**" means an individual container created within the Portal representing an audit scope (e.g. report) and/or technical scope.
- **"Data Source"** means 1 account configured for any plugin supported via the Automation module. For example, a plugin with 4 accounts will be counted as 4 data sources. As another example, 2 plugins each having 2 accounts will be counted as 4 data sources.
- **"Corporate Controls Environment"** means 1 Program used to manage a central or corporate environment, intended to be combined with more specific Programs dedicated to more targeted environments, business units, or other scopes.
- **"Program with Automation"** means a Program on which Automation Module plugins may be enabled and connected. For example, if Client has licensed 3 Programs with Automation and Client has 10 total Programs, that means 3 of those Programs may have Automation Module plugins enabled on them and 7 of them may not have Automation Module plugins enabled. Each Program with Automation may have 20 Data Sources, plus any additional quantity of Data Sources as identified in the Order Confirmation.

4: Additional Terms and Disclosures

- **Framework License Requirement and Indemnification.** The Service provides functionality incorporating various Information Security Framework Standard texts which may be public domain or may be text licensed from third parties. These texts may only be displayed and/or enabled in the Service by validly licensed users according to their separately obtained license agreements with the licensing authority. Client agrees to only enable, display, or otherwise use Information Security Framework Standards and/or text for which Client has obtained the required rights. Client will indemnify, defend and hold Coalfire, its parents, subsidiaries, Affiliates, successors, and their directors, officers, employees, agents and representatives (collectively the "**Indemnified Parties**") harmless, from and against any and all third party claims, demands, lawsuits, judgments, fines, and penalties (including interest thereon and court costs) caused by a claim that any Client does not have sufficient rights and/or licenses to use the Information Security Framework Standards and/or text in connection with the Service. ISO 27001 framework use requires that Client has licensed 27001, 27002, and 27003.
- **No Reverse Engineering. Customer shall** not, directly or indirectly, reverse engineer or aid or assist in the reverse engineering of all or any part of the Service, including without limitation, any evidence mappings of any provided framework, or otherwise deriving source code and/or evidence and/or framework data.

5: Client Assistance and Technical Support

Client Assistance

Coalfire will provide the following assistance as part of the Service, during regional business hours:

- Receive and process orders for implementation of the Service
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions

Technical Support

If Coalfire is providing Technical Support to Client, Technical Support is included as part of the Service as specified below. If Technical Support is being provided by a reseller, this section does not apply.

- Support is available during Normal Business Hours to assist Client with configuration of the Service features and to resolve reported problems with the Service.
- Once a severity level is assigned to Client's submission for Support, Coalfire will make every reasonable effort to respond per the response targets defined in the table below during Normal Business Hours.
- The Support Response and Update Targets are attainable during normal service operations and do not apply during Maintenance to the Service and/or supporting infrastructure as described in the Maintenance section below.
- Issues originating from Client actions or requiring the actions of other service providers are beyond the control of Coalfire and as these issues are specifically excluded from this Support commitment. Response and Update targets are not commitments for resolution.

Problem Severity	Support Response Target	Support Update Target
Severity 1: A problem has occurred where no workaround is immediately available in one of the following situations: (i) Customer's production server or other mission critical system is down or has had a substantial loss of service; or (ii) a substantial portion of Customer's mission critical data is at a significant risk of loss or corruption.	8 Hours	Every 48 Hours
Severity 2: A problem has occurred where a major functionality is severely impaired. Customer's operations can continue in a restricted fashion, however long-term productivity might be adversely affected.	2 Days	Every 4 Days
Severity 3: A problem has occurred with a limited adverse effect on Customer's business operations.	4 Days	1 Time / Week

Maintenance to the Service and/or supporting Service Infrastructure

Coalfire must perform maintenance from time to time. The following applies to such maintenance:

- **Planned Maintenance:** Planned Maintenance means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. For Planned Maintenance, Coalfire will provide seven (7) calendar days' notification posted on Coalfire Status.
- **Unplanned Maintenance**: Unplanned Maintenance means scheduled maintenance periods that do not allow for seven (7) days notification and during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. Coalfire will provide a minimum of one (1) calendar day notification posted on Coalfire Status. During Unplanned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. At times Coalfire will perform Emergency Maintenance. Emergency Maintenance is defined as maintenance that must be implemented as quickly as possible to resolve or prevent a major incident. Notification of Emergency Maintenance will be provided as soon as practicable.

6: Definitions

Administrator	means Client's designated personnel to manage the Service on behalf of Client.
Availability	means access to the core features of the Service that are available to the Internet minus any Excused Outages, during a calendar month.
Information Security Framework Standard	means a written set of information security related requirements, the text of which may be in the public domain (such as NIST SP 800-53 Rev. 4), or they may be licensed from an entity (such as ISO/IEC 27001:2013).
Non-Excused Outage	means the number of minutes that the Service is not available that are not an Excused Outage
Normal Business Hours	means Monday through Friday, 8:00 am – 8:00 pm US Eastern Time, excluding U.S. public holidays.
Service Credit	means the number of days that are added to Client's current Subscription Term.
Service Infrastructure or Infrastructure	means any Client or licensor technology and intellectual property used to provide the Services.

End of Service Description