ACCEPTANCE

By executing a Coalfire Service Order with reference to, and the incorporation by reference of, the terms located at https://www.coalfire.com/documents/agreements/requirements-and-assumptions, Client hereby agrees that the terms and conditions set forth in this document that are effective as of the Effective Date of the Service Order govern Coalfire's delivery and Client's receipt of the applicable Service(s) of Coalfire.

GENERAL TERMS AND CONDITIONS

CHANGE ORDERS	• If Coalfire determines that a modification to the Engagement Scope is appropriate, such modification will be reflected in a change order ("Change Order") that is executed by the Parties. A Change Order may result in a change to the fees listed. • If the Parties cannot agree on the terms of a Change Order, then notwithstanding the terms of the Agreement, Coalfire may terminate this Service Order.
TIME AND MATERIALS SERVICES	• The number of hours allotted for time and materials Services may not be sufficient to provide the Services in the Engagement Scope. If Coalfire determines that additional hours are required to perform such Services, Coalfire will notify Client in writing and the Parties will work in good faith to negotiate and execute a Change Order. • If Coalfire exhausts the total not-to-exceed hours, then Coalfire will cease providing those Services to Client. Client shall forfeit any not-to-exceed hours that are not used within twelve (12) months of the Effective Date ("Utilization Period"). • Client understands that the number of hours allocated to perform Service(s) may include up to two (2) hours of project management activities. • Fees for pre-paid time and materials Services are payable as of the Effective Date. Client shall use all pre-paid time and materials Services within the Utilization Period. Client shall forfeit any fees that were pre-paid for time and materials Services that are not used within the Utilization Period. After the expiration of the Utilization Period, the Parties may enter into a new Service Order. Services are subject to Coalfire's then-current rates.
INVOICING, TRAVEL & EXPENSES	• Coalfire will honor the prices listed in a Service Order for thirty (30) days from the date of the Service Order. • For fixed-fee Services, Coalfire will issue invoices to Client in accordance with the terms of the Agreement. Amounts paid for fixed-fee Services are not transferable to any other Service that Coalfire may provide to Client beyond the Service Order. • For time and materials Services, Coalfire will issue invoices to Client monthly, in arrears. • Coalfire will invoice Client for travel and other related expenses which are not expressly set forth in this Service Order in accordance with Coalfire's Travel and Expense Policy. • If significant delays occur in the achievement of invoicing milestone, Coalfire may issue a progress invoice covering the level of effort and associated fees for Services completed to the date of the invoice.
MISCELLANEOUS	• Notwithstanding the terms of the Agreement, any purchase order or other document issued by Client will be effective only to confirm mutually agreed upon Services, Deliverables, and fees. Any legal terms or conditions on such purchase order or document will be of no effect. • Any outcome of the Services is limited to a point-in-time examination of Client's Engagement Scope. • Coalfire relies upon accurate, authentic, and complete information provided by Client. • Client shall notify Coalfire if it has had or becomes aware of any system breach or compromise related to its business processes or any system it owns or manages during Service delivery. • Client will cooperate with Coalfire and take all actions reasonably necessary to enable Coalfire to perform the Services. To that end, Client will provide, on a timely basis, all information, as well as access to systems, locations and personnel, requested by Coalfire to enable Coalfire to provide the Services. • Notwithstanding the terms of the Agreement, either Party may terminate this Service Order at any time and for any reason upon thirty (30) days' notice to the other Party. In the event of such

GENERAL TERMS AND CONDITIONS	
	termination, Client shall pay Coalfire for all Services rendered and expenses incurred prior to the effective date of such termination. • Time and Materials Services, remediation support or re-testing that are not expressly identified herein will be delivered subject to written agreement between the Parties. • Client shall be responsible for paying round trip shipping expenses associated with the shipment and return of equipment required for technical testing, if any. • Multi-year pricing assumes no significant changes to the Engagement Scope or changes to a requesting organization's, government authority's, or industry body's testing and reporting guidance that are relevant to the Services. If Coalfire determines that a modification is required to perform the Services, the Parties will work in good faith to negotiate and execute a Change Order. The Parties agree that project activities and the associated budget may be revised accordingly. Coalfire agrees to give Client thirty (30) days' written notice of any increase in pricing.

SERVICE-SPECIFIC TERMS AND CONDITIONS	
Cyber Risk	• Client will provide all requested information, including interviews, documentation, work papers, artifacts, and feedback on Deliverables in accordance with agreed-upon timelines defined during project charter. • All Deliverables are provided to Client as point-in-time drafts. Once Client has had the opportunity to provide feedback in accordance with the timelines agreed to in the project charter, Coalfire will revise and update the documents and deliver an updated, final copy of the Deliverables. Note that any longer-term documentation updates required due to long-term remediation efforts, untimely Client review, or feedback originating from external assessment activities and other factors will require the initiation of a separate task and additional cost for those documentation updates. • Coalfire will not assume any responsibility for the Deliverables once final drafts are submitted and the Deliverables are no longer controlled by Coalfire as part of the engagement activities. • During the Services, Client shall ensure that no significant changes occur to the environment that is described in the Engagement Scope. • In the event there are T&M tasks within this Service Order, Coalfire will require written authorization from the Client prior to beginning each T&M task within this Service Order.
FedRAMP Assessment	• Coalfire will follow the latest authoritative templates required to successfully assess the Client as of the Effective Date. Depending on the applicable requirements, these may be Coalfire-managed templates or may be dictated by an external body (i.e. sponsoring agency or entity, FedRAMP PMO, CMS, etc.). • Coalfire will not perform any FedRAMP advisory activities under this Service Order. • Coalfire and Client shall not send sensitive documents to the other Party via e-mail. • During the Assessment, Client shall ensure that no significant changes occur to the environment. • Coalfire does not guarantee Client will be granted an initial or continuing authorization to operate (ATO) upon the completion of the assessment. • Client shall provide all requested security documentation to Coalfire in accordance with agreed-upon timelines defined during project charter. • If vulnerability scanning is in-scope, vulnerability scanning tools will be provided by the client. Client is responsible for ensuring all administrative privileges are working to all authenticated scans of all in-scope devices and IP addresses. Coalfire will oversee the official scans that are run and will analyze the results. • If penetration testing is in-scope, penetration testing services will not occur until after the ROE has been finalized and signed by both Parties. • Security control testing will be performed on all in-scope security controls defined in the applicable requirements.

SERVICE-SPECIFIC TERMS AND CONDITIONS	
	• Retesting and re-validation of identified findings is not within the Engagement Scope unless specifically defined as such in the Service Order. • Any security control testing required by the sponsoring agency or entity that exceeds the level of testing defined in the applicable requirements will require a Change Order for the additional level of effort to test those security controls and requirements. • The Parties acknowledge that changes to the applicable requirements which are implemented after the Effective Date may affect how Coalfire performs the Services. If changes to the applicable requirements occur after the Effective Date, the Parties agree to jointly review the changes and may agree to execute a Change Order to reflect the adjustments in Services, Deliverables, and fees listed herein.
FedRAMP Advisory	• Client will provide all requested information, including interviews, documentation, work papers, artifacts, and deliverables in accordance with agreed-upon timelines defined during project charter. • All Deliverables are provided to the client as point-in-time drafts. Once Client has had the opportunity to provide feedback in accordance with the timelines agreed to in the Project Charter, Coalfire will revise and update the draft Deliverables and deliver a final copy of the Deliverables to Client. Note that any longer-term documentation updates required due to long-term remediation efforts, untimely Client review, or feedback originating from 3PAO assessment activities and other factors will require the initiation of a separate task and additional cost for those documentation updates. • Client will review and provide feedback on all Deliverables in accordance with agreed-upon timelines defined during Project Charter, not to exceed four weeks from receipt. • Coalfire will not assume any responsibility for the Deliverables once final versions are submitted and the Deliverables are no longer controlled by Coalfire. • Client represents that the information system boundary in the Engagement Scope will not significantly change during the engagement. Client understands and agrees that any changes to the information system boundary may necessitate a Change Order and budget modification. • In the event there are Services being billed on a time and materials basis within this Service Order, Client must provide written authorization to Coalfire before Coalfire begins each time and materials Service. • Notwithstanding the terms of the Agreement or any confidentiality agreement between the Parties, Coalfire may publish Client's name on the FedRAMP.gov website, thereby disclosing Coalfire's relationship with Client as a service provider.
Incident Response	• If Coalfire exhausts the total not-to-exceed Incident Support Hours provided above, then Coalfire will cease providing those Services to Client. Client shall forfeit any not-to-exceed Incident Response hours that are not used within thirty-six (36) months of the Effective Date. • The Incident Response Services purchased under this Service Order shall have the initial term as set forth above, and if no term is stated, the Services shall have a term of one (1) year ("Initial Term"). Upon expiration of the Initial Term, this Service Order shall automatically renew for successive terms of one (1) year at the prices listed herein, unless either Party provides notice of non-renewal no later than thirty (30) days prior to the expiration of the Initial Term or any successive renewal term(s). • Upon the anniversary date of the Initial Term or any successive renewal term(s), Coalfire will invoice Client for the annual subscription fee. • Except those disclosed to Coalfire, the Client represents that it is unaware of any previous, on-going or potential data breach or compromise related to its business processes or any system it owns or manages. Client agrees to notify Coalfire if it becomes aware of any such breach or compromise during Service delivery. • The Incident Response Services may be renewed a maximum of two (2) times after the Initial Term. • Disk drives and other storage media may be required to collect data and preserve potential evidence for future action, including incident response and litigation. Client agrees to reimburse Coalfire at Coalfire's costs for such disk drives required for this purpose.
Forensics	• Services will be rendered, and Deliverables provided on a schedule agreeable to the Parties.

SERVICE-SPECIFIC TERMS AND CONDITIONS	
	• Disk drives may be required to collect data and preserve potential evidence for future action, including incident response and litigation. Client agrees to reimburse Coalfire at Coalfire's costs for such disk drives required for this purpose.
Penetration Testing	• Coalfire may use various commercial, open source, freely distributed or proprietary testing tools, techniques and monitoring methods to evaluate the devices, software or resources within the penetration testing Engagement Scope. Coalfire may also use tools that meet the definition of malware by anti-virus platforms. Coalfire is not responsible for adverse consequences resulting from inaccurate information, including inaccurate IP Addresses, furnished by Client with respect to any devices, software or resources within the penetration testing Engagement Scope. • All testing activities performed by Coalfire Labs are conducted between 6:00AM and 6:00PM Mountain Time, Monday thru Friday, national holidays excepted. Any testing required outside of this timeframe and not specified in this Service Order shall be set forth in a Change Order and subject to an additional charge of 20% of the total amount due for Penetration Testing. • For mobile application penetration testing, client is responsible for ensuring installation packages are in working order and available either on the platform marketplace or as a separate install package provided by the client. • PCI DSS requires remediation retesting be performed for all vulnerabilities identified as requiring remediation. Remediation retesting is done on a T&M basis, specifically scoped based upon the vulnerabilities to be re-tested.
CoalfireOne® and Scans	• If applicable, the terms and conditions located at the following link shall govern Client's use of Coalfire's CoalfireOne® computer program: http://www.coalfire.com/CoalfireOne-MSA. • Notwithstanding anything in any agreement between the Parties to the contrary, Coalfire may submit the scan report, along with any clarifying notes, documents, or verbal input, to the card brands or Client's acquiring bank/processor in accordance with practices adopted by the Payment Card Industry ("PCI") Security Standards Council ("SSC"). • The Services purchased under this Service Order shall have the initial term as set forth above, and if no term is stated, the Services shall have a term of one (1) year ("Initial Term"). Upon expiration of the Initial Term, this Service Order shall automatically renew for successive terms of one (1) year at Coalfire's then-existing rates and fees, unless either Party provides notice of non-renewal no later than thirty (30) days prior to the expiration of the Initial Term or any successive renewal term(s). • CoalfireOneSM Lighthouse™ Return Policy - In the event Client's CoalfireOne℠ internal scanning Service is terminated, Client shall return the CoalfireOne℠ Lighthouse™ equipment within thirty (30) days of the effective date of Service termination. If Coalfire does not receive the Lighthouse™ equipment in that time period, then Coalfire will send Client an invoice for the value of the equipment, and Client shall pay the invoice promptly. If the CoalfireOne℠ Lighthouse™ equipment is lost, damaged or are otherwise unable to be returned in working condition, Coalfire will invoice Client for the full replacement cost.
SAO	• Client is solely responsible for the procurement of and payment for services and/or licenses that are required to implement any third-party services within the deployed system. • Notwithstanding the terms of any other agreement between the Parties, Client understands that Coalfire will use its existing knowledge, training, experience, code, software, technology and proprietary methodologies to perform the Service and may develop the same during its performance of the Service ("Coalfire IP"). Client will not acquire, and Coalfire will not assign, any right, title or interest in or to the Coalfire IP or any text, data or other materials that were licensed to Coalfire to enable Coalfire to perform the Service or to create the Deliverables ("Third-Party IP"). As between Coalfire and Client, Coalfire is and will remain the owner of all Coalfire IP or licensee of all Third-Party IP. Coalfire hereby grants to Client a revocable, non-exclusive, and royalty-free license to use Coalfire IP for Client's internal business purposes and is strictly prohibited from using Coalfire IP for commercial or financial gain. • Deliverables are provided to Client as point-in-time drafts. Client must provide feedback to Coalfire by the date agreed upon by the Parties in the Project Charter and/or project schedule. Upon receipt of Client's feedback, Coalfire will update the Deliverable and provide a final copy of the Deliverable to Client. Updates to documentation due to client activities that extend beyond agreed upon timelines, untimely feedback, or feedback originating from an assessment may result in additional work and cost.

SERVICE-SPECIFIC TERMS AND CONDITIONS	
	• Client is required to perform regression testing on its application and/or technical solution before the application is deployed in the environment built by Coalfire under this Service Order. Client acknowledges that Coalfire is not responsible for any application incompatibilities outside of Coalfire's control, and therefore, Client hereby waives any claims against Coalfire with respect to same.
ASV IP Address	• With respect to Coalfire's PCI Assessment Services, no action arising out of this Agreement, regardless of the form, may be brought by either Party more than 12 months after the cause of action has accrued, except for actions with respect to non-payment. • Coalfire has no liability for actions by Visa U.S.A., PCI or PCI's member organizations, their employees, officers, consultants, subcontractors or affiliates with respect to Client's confidential information contained in the any formal compliance attestation report subject to standards published by the PCI SSC (including, but not limited to, Report on Compliance, Report on Validation, ASV Vulnerability Scan Report, and other developed materials).
PCI	• Except as identified to Coalfire in writing, Client represents that it periodically examines systems for retention or transmission of unencrypted credit card data, including track data, and Client represents that it does not store such unencrypted data. • The Parties acknowledge that changes to the Payment Card Industry ("PCI") Data Security Standard ("DSS") or PCI Forensic Investigation ("PFI") requirements which are implemented after the Effective Date may affect how Coalfire performs the Services. If changes to the PCI Security Standards Council ("SSC") or PCI PFI requirements occur, the Parties agree to jointly review the changes and may agree to execute a Change Order to reflect the adjustments in Services, Deliverables, and fees listed herein. • Any Coalfire services performed around undocumented cardholder data flows will constitute additional out-of-scope work and is not covered by the fees section of this Service Order. • During this engagement, Coalfire may identify third-party entities connecting to the Client's network. Data flows transferred over these connections are in-scope, but assessments of vendor networks or systems on the other end of these connections are not included in this Service Order. • Client is responsible for fees payable to the PCI SSC or card brands related to the Services. • With respect to Coalfire's PCI Assessment Services, no action arising out of this Agreement, regardless of the form, may be brought by either Party more than 12 months after the cause of action has accrued, except for actions with respect to non-payment. • Coalfire has no liability for actions by Visa U.S.A., PCI or PCI's member organizations, their employees, officers, consultants, subcontractors or affiliates with respect to Client's confidential information contained in the any formal compliance attestation report subject to standards published by the PCI SSC (including, but not limited to, Report on Compliance, Report on Validation, ASV Vulnerability Scan Report, and other developed materials). • Client agrees that Coalfire may submit project Results to a Requesting Organization, as those terms are defined by the PCI Security Standards Validation Requirements for Qualified Security Assessors. • The Results may include a Report on Compliance and, without limitation, any associated working papers, notes, and other materials and information generated in connection with this project, including a copy of this Agreement. • The Results may include a Report on Validation and, without limitation, any associated working papers, notes, and other materials and information generated in connection with this project, including a copy of this Agreement. • Client must complete an assessment using CoalfireOneSM Rapid PA-DSS. Per PCI DSS guidelines, the Implementation Guide must be complete before the PA-DSS Assessment Phase can be started.
GDPR	• Notwithstanding the terms of the master agreement between the Parties, Coalfire shall have no indemnification obligations arising out of or related to its delivery obligations under this Service Order or with respect to any Deliverable provided to Client hereunder. Furthermore, in no event shall the liability of either Party exceed the amount of fees payable by Client to Coalfire under this Service Order.

SERVICE-SPECIFIC TERMS AND CONDITIONS	
PCI Forensic Investigation	• Client acknowledges that all Deliverables are subject to review and acceptance by the Participating Payment Brand(s) and may be rejected for any reason. If a Deliverable is rejected, Coalfire and Client shall cooperate to resolve any discrepancies and revise the Deliverable in a timely manner. Coalfire will provide the foregoing services on a time and materials basis, and Client agrees to pay Coalfire's then-current rates for such services as invoiced by Coalfire. • Notwithstanding anything in the Agreement or a confidentiality agreement, Coalfire may provide all final and draft Deliverables and work papers to affected Participating Payment Brand(s) and acquirers as required in the PFI Program Guide without further authorization from Client. Additionally, Client acknowledges and agrees that the Services are being performed as part of the PFI Program, and all Deliverables and applicable information will be shared with affected Participating Payment Brand(s) throughout the Services. The Services are not to be directed or controlled in any way by Client or Parties acting on behalf of Client. • Notwithstanding anything in the Agreement or a confidentiality agreement, Coalfire may retain all evidence, work papers, and Deliverables related to these Services for at least one (1) year following the dissemination date of the Final PRI Report unless required by applicable law of the region/country in which the security issue occurred. • Client understands that it is an "Entity Under Investigation" as that term is defined in the Payment Card Industry PCI Forensic Investigator Program Guide, Version 3.0, (as amended) and agrees to adhere to all requirements and responsibilities attributable to an Entity Under Investigation more fully described therein. • In the event Coalfire is required to comply or respond with an order, subpoena or requirement of a court, administrative agency, governmental body or dispute resolution organization in any legal action involving Client, Client will pay the attorneys' fees of Coalfire and the regular hourly fees of Coalfire personnel in complying or responding with such order, subpoena or requirement. • Notwithstanding the terms of the master agreement between the Parties, Coalfire shall have no indemnification obligations arising out of or related to its delivery obligations under this Service Order or with respect to any Deliverable provided to Client hereunder. • Notwithstanding the terms of the master agreement in effect between the Parties, if any, or any of the terms stated herein, neither Coalfire NOR its employees, officers and directors and licensors (including without limitation the Payment Card Industry ("PCI") Security Standards Council ("SSC")) will be liable to CLIENT for commercial loss OR lost profits or any consequential, incidental, indirect, punitive or special damages, or any other similar damages under any theory of liability whether in contract, tort or strict liability, however caused and regardless of legal theory or foreseeability, directly or indirectly, arising AS A RESULT OF THE WORK PERFORMED BY COALFIRE UNDER THIS SERVICE ORDER. In no event shall THE liability under this SERVICE ORDER of Coalfire exceed the fees payable to Coalfire by Client HEREUNDER.
Healthcare	• Client agrees that failure to adhere to project charter dates including access to policies, procedures and evidence that enables Coalfire to provide the Services may result in one of the following: a. A charge to Client equal to the amount of all lost hours, billed at $250.00 per hour, but not to exceed 160 hours; or b. Client will be required to reschedule the delivery of Service, which will be dependent upon Coalfire's resource availability and may result in additional charges. • For HITRUST Validated Assessments, all testing will be completed within 90 days. Any MyCSF access extensions beyond such 90-day period may be subject to an additional charge of $500.00 per month.
HITRUST FastTrack Policy Development	• Client attests that a HITRUST Self-Assessment or Validated Assessment object has been created by Client that defines current in-scope control requirements. All FastTrack document development Services will be applied against those control requirements. • The client's personnel will be available for scheduled and impromptu interviews as needed with Coalfire.
HITRUST Gap Assessment	• Client attests that a HITRUST Self-Assessment or Validated Assessment object has been created by the Client that defines current in-scope requirements. All HITRUST Gap Assessment activities will be

SERVICE-SPECIFIC TERMS AND CONDITIONS	
	applied against those control requirements. Client has provided the Coalfire Assessor access to the Self-Assessment or Validated Assessment object. • Client will provide all requested RFI items by the agreed-upon RFI due date. After the agreed-upon RFI due date, Coalfire will mark any remaining missing evidence as a gap. • All control requirements will be clearly documented within the RFI workbook as to document and page number location. Any requirements no documented will be flagged as gaps unless annotated otherwise in the SO. • The client's personnel will be available for scheduled and impromptu interviews as needed with Coalfire. • Any changes to the scope of the assessment, including timeline, version change, number of requirements, or maturity levels assessed will require a change order.
Validated Assessment	• Client attests that a HITRUST Validated Assessment object has been created by Client that defines in-scope requirements. All HITRUST validation will be applied against those control requirements. Client has provided the Coalfire assessor access to the MyCSF Validated Assessment object. • All requirements scoped within a single MyCSF validated object accurately reflect the scope of the assessment. Inventories and network diagrams will accurately reflect the in-scope environment. • Any changes to the scope of the assessment, including version changes, timeline, number of requirements, number of objects to be assessed, or maturity levels assessed will require a change order. • Client will work with Coalfire to complete an accurate Organizational Overview and Scope document. Client will provide to HITRUST via MyCSF the Validated Management Representation Letter and HITRUST CSF Assurance Participation Agreement. • All HITRUST CSF requirements marked as 'Not Applicable' accurately reflect out of scope requirements and the client will provide documented justification for each Not Applicable requirement. Any in-scope requirements marked as Not Applicable will be scored as non-compliant. • Client will identify requirements where responsibility is shared with a third party and provide an accurate description for the demarcation of responsibility. • Policy and Process documentation is complete and ready to be assessed against the in-scope MyCSF controls. Any gaps identified will reduce the compliance score. • All control requirements will be clearly documented within the Pre-assessment Workbook, RFI as to document and page number location. Any requirements not documented will be flagged as gaps. • All evidence requested will be provided on time and will be clearly labeled for the complete sample set. Any evidence requests not provided or clearly labeled will be flagged as gaps. • The client will address all potential Corrective Action Plans (CAP's) directly with HITRUST. Any advice requested from Coalfire related to CAP completion will require a change order for Advisory services. • The Client's personnel will be available for scheduled and impromptu interviews as needed with Coalfire during the on-site visit and/or remotely as needed. • The Client will coordinate all onsite visits, including the scheduling of facility walkthroughs and meetings.
HITRUST Interim	• Client represents that it has a current HITRUST Validated or Certified Assessment in good standing. Client will promptly provide Coalfire with a copy of the current HITRUST Validated or Certified Assessment report. • Client attests that a HITRUST Interim Assessment object is active within HITRUST MyCSF. Client has provided the Coalfire assessor access to the Interim Assessment within HITRUST MyCSF. • All control requirements will be clearly documented within the Pre-assessment Workbook, RFI as to document and page number location. Any requirements not documented will be flagged as gaps. • All evidence requested will be provided on time and will be clearly labeled for the complete sample set. Any evidence requests not provided or clearly labeled will be flagged as gaps.

SERVICE-SPECIFIC TERMS AND CONDITIONS	
	• The client's personnel will be available for scheduled and impromptu interviews as needed with Coalfire. • Interim Assessment includes up to four (4) Corrective Action Plans (CAP's) to be assessed. Any changes to the scope of the assessment including timeline, version changes, number of CAP's, or maturity levels assessed will require a change order.
HITRUST Advisory	• A HITRUST Self-Assessment object or Validated Assessment object will be created by Client to define in-scope control requirements. All HITRUST Advisory services will be applied against those control requirements.
HITRUST Workshop	• A sample of the client's policy and procedure documentation based on RFI will be provided prior to the workshop to support the "Policy & Procedure Review Exercise" workshop activity. • The sample control requirements will be clearly documented within the RFI as to document and page number location. Any requirements not documented will be flagged as gaps for discussion. • The Client will coordinate all onsite visits, including the scheduling meetings with the following organizational personnel: Chief Information Officer, Chief Privacy Officer, Chief Security Officer, VP of Technology, VP of Information Security, Director/Manager of Information Security, Director/Manager of Technology, Senior System Administrators.
HIPAA Security Risk Analysis	• Client agrees that Coalfire will provide all reports and worksheets (draft and final) in a read-only format to ensure integrity of the assessment and resultant findings. • Client agrees that any 3rd Party penetration tests, vulnerability assessment reports and other security testing results will be made available to Coalfire for reference during the Risk Analysis. • Client agrees that implementation of controls / activities / configurations to mitigate the findings is the responsibility of the client, unless specifically included in the scope of this Service Order.
ISO Certification Audit	• If the Services requested by Client in any Service Order include ISO/IEC 27001:2013 Certification or associated services as described below, the following additional provisions shall apply: a. For purposes of Client certification to ISO/IEC 27001:2013 and in compliance with section 5.1.2 of the ISO/IEC 17021-1:2015 standard, this agreement is a legally enforceable agreement between CFISO and the client. In addition, where there are multiple offices of CFISO or multiple sites of the Client, this agreement is between all CFISO sites as the body granting certification and issuing a certificate and all Client related sites covered by the scope of the certification. b. At all times during the operation of this agreement, Client agrees that CFISO is responsible for, and will retain the authority for, its decisions relating to certification, including granting, maintaining, renewing, extending, reducing, suspending, and withdrawing of certification. c. If CFISO agrees to issue certification of the Client ISMS, for purposes of conformance to the ISO/IEC 27001:2013 standard, Client agrees that it: i. Will inform CFISO, without delay, of matters that may affect the capability of the management system to continue to fulfill the requirements of the standard used for certification. ii. Will conform to the requirements of CFISO when referring to its certification status in communication media such as the internet, brochures or advertising, or other documents and including the use of the CFISO certified mark as set out in the certification documentation. iii. Will not make or permit any misleading statement regarding its certification. iv. Will not use, or permit the use of, a certification document or any part thereof, or the CFISO certification mark in a misleading manner. v. Will, upon suspension or withdrawal of its certification, discontinue its use of the CFISO certified mark and all advertising matter that contains a reference to certification, as directed by CFISO.

vi. Will amend all advertising matter when the scope of certification has been reduced.

vii. Will not allow reference to its management system certification or use the CFISO certification mark in such a way as to imply that the certification body certifies a product (including service) or process and will not allow reference to certification or the CFISO mark in connection with any laboratory test, calibration, or inspection reports, as such reports are deemed to be products in this context.

viii. Will not imply that the certification applies to activities that are outside the scope of certification.

ix. Will not use its certification in such a manner that would bring the certification body and/or certification system into disrepute and lose public trust.

x. Understands that CFISO shall always exercise proper control of ownership and shall take action to deal with incorrect references to certification status or misleading use of certification documents, marks, or audit reports and that such action could include requests for correction and corrective action, suspension, withdrawal of certification, publication of the transgression, and, if necessary, legal action.

xi. Understands that under suspension, the client's management system certification is temporarily invalid.

xii. Will, if notified by CFISO that its management system is under suspension, agree to refrain from further promotion of its certification and that CFISO shall make the suspended status of the certification publicly accessible and shall take any other measures it deems appropriate.

xiii. Agrees and acknowledges that failure to resolve the issues that have resulted in the suspension in a time established by the CFISO must result in withdrawal or reduction of the scope of certification. (Note: In most cases, the suspension would not exceed 60 days).

xiv. Will, in the event of withdrawal or reduction in scope of certification, discontinue its use of all advertising matter that contains any reference to a certified status.

xv. Acknowledges and accepts that, upon request by any Party, CFISO must correctly state the status of certification of a client's management system as being suspended, withdrawn, or reduced.

xvi. Acknowledges and accepts that, upon CFISO receiving a complaint about the client certification, CFISO is responsible for gathering and verifying all necessary information to validate the complaint and whatever else should the client be notified about in the agreement.

xvii. Shall agree to make available to CFISO, when requested, the records of all complaints and corrective action taken in accordance with the requirements of ISO/IEC 27001:2013.

xviii. Accepts and acknowledges that CFISO will determine, together with the client and the complainant, whether, and if so to what extent, the subject of the complaint and its resolution is made public

Certification of Compliance and Digital Seal

- Certificate of Compliance. The following terms shall apply to the Services provided by Coalfire to Client hereunder, notwithstanding the terms of any other agreement between the parties:

  a. "Seal" means an electronic image featuring Coalfire's mark intended for display on any Coalfire-approved domain.
  b. Coalfire hereby grants to Client a nonexclusive, non-transferable, revocable, non-sublicensable license during to display Seal on its website.
  c. Client may not: 1) copy, sell, rent, lease, transfer, assign or sublicense the Seal, in whole or in part, or alter the Seal in any way; or 2) take any action that would interfere with or diminish Coalfire's intellectual property rights in the Seal.

SERVICE-SPECIFIC TERMS AND CONDITIONS	
	d. Coalfire reserves the right to remove the Seal from Client's website and this Service Order shall automatically terminate, if: i. Coalfire discovers that the information that Client provided during Coalfire's performance of Coalfire services was inaccurate, incomplete, misleading, or no longer valid; ii. Client violates any of the restrictions set forth in this Service Order; iii. Client uses the Seal for any unlawful purpose. e. Upon termination of this Service Order or expiry of any applicable compliance period, Client shall immediately cease its use of display of the Seal and shall not use the Seal for any purpose thereafter. • Digital Seal. Subject to the terms of the Service Order, the seal is valid for the same period of time as the successful scan, assessment, or validation addressed in the linked Certificate of Compliance. a. Digital Seals may only be displayed on approved domains associated with the organization that achieved compliance; b. The Client listed above has engaged Coalfire in its information security program in accordance with commonly accepted best practices. If the "scan" certificate is displayed, no significant vulnerabilities were found as of the last successful scan date. In all circumstances, the Client acknowledges and agrees that thy outcome of such scan, assessment or validation effort is a point-in-time examination. Coalfire makes no representations, warranties or claims of any kind, regarding the information of service provided or the Client's business activities or operations. In addition Coalfire does not guarantee that the Client's web site or systems are immune from hackers or secure from either an internal or external attack, that any data is free from risk of being compromised, or that any data stored on the Client's systems or site is safe, and Coalfire is in no way responsible for the security of or use of any of the information stored on a scanned site.
Public Relations & Communication Support	• Press Release a. Coalfire does not pay for wire distribution of media pitching. Client is responsible for managing press release distribution; b. Coalfire will provide a review of your final, approved content, with up to one additional review of revised content if needed. • Social Media Coverage a. Limit to one template design for LinkedIn and Twitter; b. Limit to 2 suggested posts for LinkedIn and Twitter; c. Client is responsible for posting to their own social platforms; d. 48-hour turnaround time to account for customization.
Webinar Support	• Client's organization will host webinar with their web conferencing platform. Coalfire will assist in developing a storyboard and project plan, support content development, participate in a practice session, and provide additional promotion through Coalfire social media channels. Coalfire will promote via social media posts only; Coalfire will not send emails to our database about the webinar. Coalfire will provide up to 58 hours of webinar support.
Sales Data Sheet	• Coalfire will provide writing, editing, and layout services for up to two rounds of revisions, and the Coalfire logo for use within the document. Coalfire will not provide native (or editable) files, nor print copies for client. a. The Coalfire team will work with the client to complete projects within the scope of work detailed previously. In the event that a project changes in scope, additional rounds of revisions are needed, new elements are introduced, etc., the parties will discuss any changes and create a change order for the parties' approval. b. The document will co-branded by both Coalfire and your organization and available for use by your marketing and sales terms.

SERVICE-SPECIFIC TERMS AND CONDITIONS	
Sales Call Support and Thought Leader Event Support	• Sales Call Support and Thought Leader Event Support. Up to 1.5 hours maximum SME time for each requested sales call. Coalfire will provide writing, editing, and layout services for up to two rounds of revisions, and the Coalfire logo for use within the document. Coalfire will not provide native (or editable) files, nor print copies for client. • Event Support. Client will be responsible for travel expenses.