

# Incident Response Retainer Services

## Service Description

May 2020

### SERVICE OVERVIEW

This Service Description is provided under the following terms and conditions in addition to any terms and conditions referenced in the order confirmation issued by Accenture (or Symantec, as predecessor to Accenture) related to Customer's purchase of Services or any similar document which further defines Customer's rights and obligations related to the Services, such as a Symantec certificate (the "**Order Confirmation**") which incorporates this Service Description by reference (the Order Confirmation, this Service Description and any other documents referenced therein collectively, the "**Agreement**"). Any terms that are used but not defined herein shall have the meaning set forth in the Agreement. This Service Description shall apply to Services purchased by Customer on or after May 1, 2020. For Services purchased by Customer prior to May 1, 2020, the version of the Service Description that applies is based on Customer's purchase date, a copy of which is available at [www.accenture.com/us-en/insights/security/legal-terms](http://www.accenture.com/us-en/insights/security/legal-terms) or upon request to Accenture.

Incident Response Retainer Services allow Customer to engage Accenture to provide incident response and investigation services, as described in more detail herein (the "**Services**"). Upon request from Customer in accordance with the process set forth below, Accenture will provide resources to perform the Services. Services will be provided at the hourly rates as set forth in the Order Confirmation. All Services **must** be delivered by Accenture within the countries set forth in the Order Confirmation or Work Authorization Form (as defined below).

# Incident Response Retainer Services

## Service Description

May 2020

### SERVICE FEATURES

SERVICE FEATURE	SERVICE FEATURE DESCRIPTION
<b>24x7 PHONE AND EMAIL ACCESS</b>	Customer will have access to a 24x7 phone number to contact the Incident Response delivery team to request incident response assistance (“ <b>Incident Response Assistance Call</b> ”). Customer may also contact the Incident Response delivery team 24x7 by email at <a href="mailto:CIFR.hotline@accenture.com">CIFR.hotline@accenture.com</a> .
<b>CALL-BACK SLA</b>	The Incident Response delivery team will return Customer’s Incident Response Assistance Call within 2 hours following receipt of such call by Accenture. In the event Customer’s Incident Response Assistance Call is not returned within the applicable timeframe, Accenture agrees to credit Customer’s account with 1 Service Credit.
<b>EMERGING THREAT REPORTS</b>	Accenture will periodically provide Customer with emerging threat reports published by Accenture via email on emerging threats that may impact Customer’s security posture.
<b>INCIDENT INVESTIGATION</b>	An overview of the activities Accenture may perform during an Incident Investigation are provided below under “ <b>INCIDENT INVESTIGATION</b> ”. An Incident Investigation shall be performed at Customer’s location, which must be within the country or countries set out in the Order Confirmation or agreed by the parties in the Work Authorization Form.
<b>FEES</b>	<p>Customer is responsible for to pre-pay the retainer fee (“the Retainer Fee”) set forth in the Order Confirmation. The Retainer Fee is non-refundable. Where Customer engages Accenture to provide Services, Accenture will credit against the Retainer Fee using the hourly rates set forth in the Order Confirmation for time actually spent.</p> <p>In the event that the Retainer Fee is exhausted, any additional Services will be billed on a time and materials basis at the hourly rates set forth in the Order Confirmation. In the event that the Retainer Fee is not exhausted, then the parties may agree that such remaining fees can be used toward IR consulting services, as described below.</p>
<b>Fly to Site SLA (within US)</b>	An Accenture resource will be “in transit” to Customer’s U.S. location for an Incident Investigation within 24 hours following Incident Investigation Registration. The term “in transit” means the Incident Investigation responder(s) will have commenced travel to Customer’s location, which <b>must</b> be within the <u>United States</u> . In the event that the Incident Investigation responder(s) is not “in transit” within the applicable timeframe, Accenture agrees to credit Customer’s account with 1 Service Credit for each Normal Work Day of delay.
<b>Fly to Site SLA (agreed locations outside of US)</b>	An Accenture resource will be “in transit” to Customer’s location for an Incident Investigation within 24 hours following Incident Investigation Registration. The term “in transit” means the Incident Investigation responder(s) will have commenced travel to Customer’s location, which <b>must</b> be within the <u>country(s)</u> for which fees have been paid as set forth in the Order Confirmation or agreed in a Work Authorization Form. In the event that the Incident Investigation responder(s) is not “in transit” within the applicable timeframe, Accenture agrees to credit Customer’s account with 1 Service Credit for each Normal Work Day of delay.

# Incident Response Retainer Services

## Service Description

May 2020

### INCIDENT INVESTIGATION

**Requesting Incident Investigation.** Customer Authorized Personnel shall contact Accenture to request an Incident Investigation. Following receipt of such notification, Accenture will schedule an initial triage call to agree next steps. Accenture will then provide Customer with a corresponding Work Authorization Form or “WAF” describing these decisions, and each party must sign the WAF to initiate the Services (“**Incident Investigation Registration**”). Incident Investigation Registration is the date of receipt by Accenture of the signed WAF. Following Incident Investigation Registration, Accenture will commence travel to Customer’s location and/or coordinate remote efforts to conduct an Incident Investigation in accordance with the Service Level Agreement (*where applicable*). Further details of what Accenture may perform during an Incident Investigation are provided below.

#### Incident Investigation Features.

Accenture will use different strategies and methodologies to complete the Services depending on the nature of the incident. Accenture will consult with Customer Authorized Personnel at the outset of the Services to identify initial objectives to be worked towards as well as regularly thereafter as to updates to those objectives and other investigation decisions as the Services progress, and Customer will make any material decisions on investigation strategy. Accenture’s Services may include Accenture utilizing the below, however Customer acknowledges and agrees that in providing the Services, Accenture may modify its approach as appropriate to assist Customer in investigating a potential security incident:

- Analysis of pertinent data / logs
- Operation of tools to collect network/ log data
- Malware analysis and reverse
- Client personnel discussions
- Incident timeline analysis

#### Remote Services:

Accenture may perform certain Services during an Incident Investigation remotely (“**Remote Service**”) on Customer data, including, without limitation, hardware, software, images, memory, network, logs (“**Customer Data**”). Customer acknowledges and agrees that any such Remote Service performed by Accenture shall be subject to the following additional terms: (a) Customer shall, at its sole cost and expense, be responsible for the delivery of Customer Data (on a medium to be mutually agreed with Accenture) to Accenture and the return of such Customer Data to Customer following conclusion of Remote Service; (b) Customer Data shall be delivered to Accenture at a location mutually agreed between Customer and the Incident Response delivery team, in a tamper-evident container (where applicable). Where applicable, Customer shall provide Accenture with the applicable delivery tracking number and shall ensure that Accenture’s physical acknowledgement of receipt is required upon delivery. For the purposes of a Remote Services, “**Accenture Receipt**” shall be the date of receipt of Customer Data by Accenture. Accenture shall have no responsibility whatsoever with respect to Customer Data, including, without limitation, to any Customer Data that may remain within any Customer hardware (whether accessible, readable or not).

#### Written Report and Presentation:

In connection with an Incident Investigation, when requested by Customer, Accenture will deliver one or more of the following documents:

- **Periodic Status Report** summarizing work done during the period
- **Remediation Plan** documenting recommended actions for remediating findings uncovered during the Incident Investigation
- **Incident Response Report** documenting pertinent data uncovered during the Incident Investigation, identifying systems compromised, and characterizing data breach-related activity and root causes if known

Upon request, Accenture may also provide a presentation summarizing the contents of the written report outlined above,

# Incident Response Retainer Services

## Service Description

May 2020

intended to be adaptable for Customer's use in briefing Customer's board of directors or senior executive staff. The proposed content of any documented reports will, where requested by Client, be discussed in advance of production or sharing. Reports typically require ten business days for production and review. The reports will be provided to the Customer Authorized Personnel and Customer's legal counsel, as applicable, and Accenture shall not be required to provide reports or documentation (or copies of them) to any other party or individual.

### IR CONSULTING SERVICES

Customers who do not exhaust their Retainer Fee during the applicable Term may request to use remaining amounts to purchase IR-related consulting services from Accenture, such as (but not limited to):

- **Incident Response Readiness Assessment Services;**
- **Incident Response Plan Assessment Services;**
- **Incident Response Plan Development Services;**
- **Incident Response Tabletop Exercises; or**
- **Incident Response Training.**

Such consulting services will not include technical assessment services, including adversary simulation or penetration testing, as such service would need to be provided under a separate arrangement.

Delivery of any such consulting services are subject to mutual agreement of the parties with respect to the scope of services and timing of delivery. Accenture will provide Customer with a corresponding WAF describing the agreed services, and Customer must sign and return the WAF to Accenture prior to the commencement of any such service. The Service Level Agreements shall not apply to any such service.

### TRAVEL AND EXPENSES ("T&E")

The Retainer Fee does not include any travel and expenses ("T&E") that may be required to deliver Services. Customer will pay, if applicable, reasonable T&E incurred in the course of performance of the Services. All T&E will be invoiced by Accenture at actual cost in accordance with Accenture's standard business practices.

### CUSTOMER RESPONSIBILITIES

Customer acknowledges and agrees that Accenture can only perform the applicable Service if Customer provides required information or performs required actions as set forth in the Agreement or as reasonably requested by Accenture. Accordingly, and without limitation, if Customer does not meet the following responsibilities, Accenture's performance of the applicable Service may be delayed, impaired or prevented, as noted below:

- **Customer Personnel.** Customer will make available personnel who have the necessary technical and business knowledge and authority to make decisions concerning the Service. In addition, Customer shall assign an appropriate number of suitable skilled personnel to assist and cooperate with Accenture consistent with the Service described in this Service Description. Customer will further provide escalation/contact information for required resources. Customer must identify and provide the names for Customer's Authorized Personnel and other Incident Response resources. Customer shall make any decisions required of it promptly and without delay and Accenture shall be entitled to rely on all such decisions and approvals.
- **Facilities.** Customer will provide Accenture with all necessary cooperation, information and support that may reasonably be required by Accenture for the performance of the Service including, without limitation, arranging and/or obtaining appropriate travel documentation (including work permits, visas, etc.), access to suitably configured computers, unrestricted network physical connectivity, technical support resources for installing network monitoring hardware, software products and applicable passwords, at such times as Accenture requests. In addition, Customer will provide Accenture personnel with access to all buildings, phone systems, internet access, server rooms, and workstations, and will provide all necessary passes for access to such areas if work is required by Customer outside of Normal Business Hours. Customer will also provide access to a suitable conference room facility for meetings, interviews, and facilitated sessions during any on-site components of the Services and provide technical support resources for installing network monitoring hardware, where applicable.

# Incident Response Retainer Services

## Service Description

May 2020

- **Information.** Customer will ensure that Accenture has access to the following at all times: (i) materials and resources related to Customer's business and technical environment; (ii) software design documentation, current design diagrams, and other information required to deliver the Service; (iii) access to all operating systems and network and computing environments necessary to complete the Service. Where applicable, such access shall include various user accounts for relevant applications, as needed, to perform for example, a penetration assessment, including, a list of relevant IP addresses, URLs and user authentication.
- While Accenture uses reasonable care to carry out the Services in a manner designed to reduce the risk of damage to Client Property (including hardware and software), Client acknowledges that there is inherent risk in the provision of security Services which may lead to operational degradation, performance impact, breach of Client's internal policies or industry standards, or otherwise impair Client Property/resources and notwithstanding any other provisions in the Arrangement Letter to the contrary, Accenture will not be liable to Client or its employees or third parties for such damage, breach or impairment arising out of provision or receipt of the Services.
- Client is responsible for notifying Accenture of any applicable export control requirements related to Client Property and obtaining any required licenses with respect to such Client Property.
- If Accenture is required to use Client tools during an engagement, Client is responsible for enabling Accenture to have appropriate access to Client-owned tools, including any necessary licenses.
- Accenture will install servers on and/or will set up capacity in Accenture or its vendor's cloud-based environment and connect to Client's network in order to collect endpoint, network and log data, and will provide Client with the hardware and software components required to be installed on Client's network and endpoint devices.

Client will:

- obtain any certificates (or modify any certificates) required to enable installation of the devices or software on any network, device or endpoint;
  - perform testing on each of its classes of devices to determine and/or confirm that the software agents do not affect reliability or availability of the devices
  - install the software agents on the agreed upon number of the Client's endpoint devices and its network in accordance with Accenture's instructions and to remove the devices or software at the end of the engagement;
- Any hardware or software provided by Accenture for installation on Clients Property ("**Accenture Tools**") remains the property of Accenture or its licensors and is subject to the additional terms set forth in the attached **Exhibit 1**.

## SERVICE-SPECIFIC TERMS

### SERVICE CONDITIONS

- **Out of Scope.** Anything not specifically described in this Service Description is out of scope and is not included in the Service.

In addition, Accenture will not provide any regulated service. Accenture is not licensed or certified in any country, state, or province as a public accountant, auditor or legal advisor, or private investigator and is not being retained to provide accounting services, accounting guidance, audit or internal control advisory services, tax or legal advice or investigatory services that would require a license.

Forensic data collection from mobile phones, tablets or e-readers is out of scope.

Customer acknowledges, understands and agrees that Accenture does not guarantee or otherwise warrant that the Service, or Accenture's recommendations and plans made by Accenture as a result of that Service, will result in the identification, detection, containment, eradication of, or recovery from all of Customer's system threats, vulnerabilities, malware, malicious software, or other malicious threats. Customer agrees not to represent to anyone that Accenture has provided such a guarantee or warranty.

# Incident Response Retainer Services

## Service Description

May 2020

- **Offsite Analysis.** Customer authorizes Accenture to perform any offsite analysis of Customer Data necessary for the Service. Accordingly, Customer acknowledges and agrees that Accenture may be required to connect its computers and equipment directly to Customer's computer network. Customer explicitly consents to Accenture connecting its computers and equipment directly to Customer's computer network and Customer assumes all risk and liability in this regard and Accenture shall have no liability in this regard whatsoever.
- **Service Hours.** Except for Customer's 24/7 access to request assistance (as described in the Service features), all Services will be performed during Normal Business Hours. However, it is understood that an Incident Investigation is provided on an urgent basis, and that flexibility may be requested and accommodated, subject to local labor laws and the free choice of the individual resources delivering the Incident Investigation.
- **Exclusions.** The following services ("**Litigation Support Services**") are explicitly excluded from the Services:
  - Depositions, fact witness testimony, expert witness testimony, affidavits, declarations, expert reports;
  - Responding to discovery requests, subpoenas;
  - eDiscovery services;
  - Other forms of litigation support or participation in any legal proceeding relating to the subject matter of the engagement (including those involving a governmental entity).

*Litigation Support Services.* Although the parties acknowledge that the Services may be sought by Customer at the direction of Customer's legal counsel, it is neither Accenture's nor Customer's intention for Accenture to perform Litigation Support Services. If, however, Accenture is later compelled to perform any Litigation Support Services, Customer and Accenture agree the following would apply to those Litigation Support Services regardless of whether such Litigation Support Services are sought directly by Customer or by a third party, and notwithstanding any conflict with other terms:

- The then-current hourly rate would apply for all Accenture personnel who perform Litigation Support Services. Litigation Support Services are provided on a time and materials basis, since the actual time required to complete Litigation Support Services may vary.
- The parties will work in good faith to document the terms in this "Litigation Support Services" section as well as any additional necessary terms and conditions in a separate agreement at such time as the need for Litigation Support Services should occur.
- This "Litigation Support Services" Section will survive termination or expiration of the Agreement.

*Privilege.* If Customer has listed General Counsel contact information in the Required Contact Information Form or has otherwise entered into a separate agreement confirming that the engagement is being conducted at the request of, and at the direction of, Customer's legal counsel, Accenture will work with all reasonable requests from Customer's legal counsel to preserve any attorney-client, attorney work product, or other applicable privileges. Accenture will treat all findings, reports and documentation it provides to Customer as part of the Services as Confidential Information.

- **Reporting.** Customer acknowledges and agrees that in the course of delivering the Services, Accenture may become aware of issues such as data breaches, network intrusions, or the presence of malware, and that such issues may give rise to regulatory reporting obligations which Customer is subject to in one of more territories in which Customer operates. Accordingly, Customer shall remain solely responsible for all such reporting requirements and Accenture shall have no liability in this regard whatsoever.
- **Personnel.** Accenture reserves the right to assign any suitable skilled resource(s) available to provide Services. Accenture is not obligated to provide a specific Accenture resource or third-party resource.
- **Consent and Authorization.** Customer agrees and authorizes Accenture to do all acts as necessary for the performance of the Services, including: (i) Access Client Property; (ii) physically connect, disconnect, install, update, upgrade, manage and operate equipment, tools and software on Client Property; (iii) to the extent required to comply with law, share information or take such actions with respect to Client Property required by law enforcement authorities or regulatory authorities (in such cases Accenture will use reasonable endeavors to the notify the Client in advance, where it is permitted by such law enforcement and/or regulatory authorities to do so); each as necessary for the performance of the Services set out in this Arrangement Letter. In addition, Customer agrees that Accenture will retain for its business purposes any indicators of compromise, malware, anomalies, or other metadata found as part of, or related to, the performance of the Services ("**Metadata**"). Accenture may analyze, copy, store, and use such Metadata in an aggregated, and de-identified manner. Accenture is performing the cyber defense Services at Customer's

# Incident Response Retainer Services

## Service Description

May 2020

request and has no intention of committing any civil or criminal offense. Customer agrees that no act or omission of Accenture arising out of or related to Accenture's provision of the Services or compliance with law, will be deemed to exceed the authorization set forth above. Customer represents, warrants and agrees that it has and will maintain all necessary rights, licenses, and Consents to authorize Accenture to perform the Services and Access the Client Property.

- **Compliance with Law.** Each party shall be responsible for compliance with laws applicable to its business. Customer shall be solely responsible for providing instructions or obtaining any necessary consents for Accenture to provide the Services in compliance with laws, including without limitation, any laws relating to network integrity or security or to data privacy or data protection.
- **Indemnity.** Customer will indemnify, save, hold harmless, and defend Accenture, its affiliates, successors, and their directors, officers, employees, agents and representatives against all claims, costs, expenses, demands, damages, regulatory fines, penalties, lawsuits, and liabilities (including, without limitation, interest, settlement amounts, legal fees and court costs) to the extent arising from or connected with any allegation or claim, whether by Customer, Customer's Employees, or a third party or relevant regulatory authority, based on: (i) the activities authorized and contemplated under this Agreement, including any claims arising out of Customer's or a third party's use of the Services; or (ii) Client's breach of its obligations under the Agreement, including this Service Description. This indemnity will survive the termination or expiration of the Agreement for any reason.
- **Service Limitation.** Applicable law or regulation(s) of the country in which Services, including without limitation an Incident Investigation, will be performed may limit or alter the scope of the Services.
- **Termination of an Incident Investigation.** Either party can terminate an Incident Investigation (but not this Agreement in whole) by providing five (5) days' notice to the other party hereunder.
- **Customer Personal Data.** In the course of an Incident Investigation, Accenture may gain access to (or obtain incidentally) Customer Personal Data. The types of Customer Personal Data that may be processed by Accenture may include (depending on the incident): personal contact information such as name, business address, business phone number, home address, home telephone or mobile number, fax number, email address, and passwords, user ids, information concerning family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, social security details; financial details including bank account data, credit or debit card data, payment or purchase history, device identifiers (such as serial numbers, mobile phone UDIDs), Internet Web Universal Resource Locators (URLs) and Internet Protocol (IP) addresses, or any other Customer Personal Data contained within the systems with respect to which the Services are provided. The Customer Personal Data transferred may concern the following special categories of data: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; data concerning health or sex life and sexual orientation; genetic data; and biometric data where processed to uniquely identify a person. The categories of data subjects involved may include any of Customer's representatives, such as employees, job applicants, contractors, collaborators, partners, and customers of the Customer. Accenture will process Customer Personal Data only for purposes described herein and in accordance with the terms of the Agreement. Customer acknowledges that it is the controller of such Customer Personal Data, and agrees that it is will take all necessary measures to ensure that it, and all of its employees or other third parties, are aware that their Personal Information may be processed as part of the Service(s) and that those individuals have given their consent to such processing, where required. Customer will comply with its responsibilities as data controller in accordance with applicable laws and/or regulations. By providing Personal Information, Customer consents, for itself, its users and contacts, to the following: Personal Information will be processed and accessible on a global basis by Accenture, its affiliates, agents and subcontractors for the purposes of providing the Service(s), to generate statistical information about the Service(s), for internal research and development, and as otherwise described in the Agreement, including in countries that may have less protective data protection laws than the country in which Customer or its users are located. Accenture may disclose the collected Personal Information as required or permitted by law or in response to a subpoena or other legal process. Customer understands and agrees that Accenture has no control or influence over the content of the Customer Personal Data processed by Accenture and that Accenture performs the Service(s) on behalf of Customer and that Accenture will only process the Personal Information in accordance with the instructions of Customer, provided that such instructions are not incompatible with the terms of the Agreement. Accenture will also take appropriate technical and organizational measures to protect personal information against accidental loss or destruction of, or damage to, that Personal Information, as set forth in Accenture's Data Safeguards, which are available upon request.

# Incident Response Retainer Services

## Service Description

May 2020

- **Conflict of Interest.** Customer acknowledges that Accenture or one of its affiliates may provide other services, such as infrastructure outsourcing, application outsourcing or business process outsourcing, to Customer or a Customer affiliate under a separate agreement. To the extent that the Services under this Agreement may raise a potential conflict of interest, Accenture will follow its internal conflict of interest processes. By engaging Accenture for any particular Services via a WAF, Customer waives any and all claims against Accenture based on a conflict of interest with respect to such Services.

## SERVICE LEVEL AGREEMENT

- A Service Credit shall equal one-half (1/2) of the applicable Standard Rate in the hourly rate table (as set forth in the Order Confirmation) for each whole hour that the SLA is not satisfied (a "Service Credit"). For example, the SLA for initial response is two (2) hours and if, due solely to Accenture, the actual response time is three (3) hours, then Accenture will issue a Service Credit equal to  $\$(0.5 \times \text{the Standard Rate}) \times 1 \text{ hour}$ . Any Service Credit applied will be Customer's sole remedy for failure to meet the SLA. If one or more SLA are missed as a result of the same underlying incident, then Service Credits will only be applied to the first SLA missed. Service Credits will be capped at 5x the Standard Rate for each failure to meet a Service Level. Service Credit(s) granted hereunder will first be applied toward Customer's next invoice due for the applicable Service after submission of a Service Credit Request, or if no additional invoice is due for the applicable Service, as a payment.
- If Customer believes it is entitled to a remedy in accordance with the Service Level Agreement, Customer must submit a Service Credit Request within 10 Normal Work Days of the end of the calendar month in which the suspected Service Level Agreement non-compliance occurred.
- All Service Credit Requests will be subject to verification by Accenture.
- Accenture shall not be responsible for its inability to perform Services (including meeting the Service Level Agreement) in whole or in part: (i) due to unforeseen circumstances or to causes beyond Accenture's reasonable control including but not limited to war, strike, riot, crime, acts of God, or shortages of resources ; (ii) legal prohibition, including but not limited to, passing of a statute, decree, regulation or order; (iii) during any period of suspension of Service by Accenture in accordance with the terms of the Agreement; (iv) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); or (v) Accenture resources are required to obtain visas prior to performing work in Customer's country.
- The remedies set out in the Service Level Agreement shall be Customer's sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise, with respect to the Service Level Agreement.

## DEFINITIONS

Capitalized terms used in this Service Description shall have the meaning given below. Any capitalized terms not defined in this Service Description shall have the same meaning as in the Agreement.

**"Accenture"** shall mean the Accenture legal entity named in the Order Confirmation. Services may be performed by Accenture or any of its affiliates, in which case the consents, authorizations and indemnities afforded to Accenture under the Agreement shall extend to Accenture affiliates who provide Services hereunder.

**"Access"** means access, attempt to gain access to, collect, use, copy, monitor, move, connect, disconnect, modify, process, transfer and store.

**"Consents"** includes all necessary consents, permissions, notices and authorizations necessary for Accenture to perform the Services, including any of the foregoing from Employees or third parties; valid consents from or notices to applicable data subjects; and authorizations from regulatory authorities, employee representative bodies or other applicable third parties.

**"Customer Authorized Personnel"** shall mean the Customer contact(s) who are authorized by customer to invoke the Services, as initially set forth in the Order Confirmation or as may be updated by Customer by providing written notice to Accenture from time to time, or, for purposes of an Incident Investigation, such other Customer contacts who may be listed in an individual WAF for that Incident Investigation.

**"Customer Property"** means computer systems; servers; technology infrastructures; telecommunications or electronic communications systems and associated communications; confidential information; data (including Customer Personal Data, employee identification, authentication or credential data user details and other sensitive information); assets; devices; intellectual

# Incident Response Retainer Services

## Service Description

May 2020

property; and/or physical premises, that are used by the Customer, its Employees, customers, or suppliers, whether owned or otherwise controlled by the Customer or owned by a third party.

“**Employee**” means employees, contractors or other users under the control of the Customer.

“**Incident Investigation**” shall mean an incident investigation conducted by Accenture based on the nature and type of a particular security incident as further described in this Service Description.

“**Normal Work Day**” shall mean a day that comprises the Normal Business Hours.

“**Normal Business Hours**” shall mean the normal working hours, typically between 8.00 a.m. and 5.30 p.m. local time, exclusive of any applicable statutory rest periods, weekends and public holidays, as observed in the country in which Services are performed.

“**Remote Assessment**” shall mean a remote assessment conducted by Accenture during an Incident Investigation as further described in this Service Description.

“**Service Credit**” shall mean the amount of money that will be refunded to Customer or credited to Customer’s next invoice after submission of a Service Credit Request and validation by Accenture that a Service Credit is due to Customer.

“**Service Credit Request**” shall mean the notification which Customer must submit to Accenture by email to Customer’s Service Manager.

“**SLA**” or “**Service Level Agreement**” shall mean the applicable service level set forth in the Service Description.

“**Order Confirmation**” shall mean one or more of the following applicable documents which further defines Customer’s rights and obligations related to the Service: a Symantec certificate or a similar document issued by Symantec (as predecessor to Accenture), an Order Confirmation document or email issued by Symantec or Accenture, or a written agreement between Customer and Accenture (as successor to Symantec), that accompanies, precedes or follows the Service.

“**Term**” shall mean the term of the subscription of the Service(s) as specified in the applicable Order Confirmation.

“**WAF**” or “**Work Authorization Form**” shall mean the form Accenture provides to Customer pursuant to which Customer authorizes and acknowledges the location, contact information, T&E, Additional Responders, Readiness Service(s), and/or Service Day(s) and/or other d for Incident Investigation(s).

**END OF SERVICE DESCRIPTION**

# Incident Response Retainer Services

## Service Description

May 2020

### **Exhibit 1 Accenture Tools Additional Terms**

The following additional terms apply in the event Accenture installs any Accenture Tool(s) on Customer's system in connection with the Services:

Accenture hereby grants Customer a non-exclusive, nontransferable, personal, limited license during the term of the applicable Incident Investigation to such Accenture Tool(s), solely to install such on Customer networks and endpoints for use in connection with the Services as applicable in accordance with instructions provided by Accenture. Unless otherwise agreed by the parties in the WAF, Customer will not otherwise have access to such Accenture Tool(s) and: (i) will prohibit its Employees from accessing such tools, (ii) may not otherwise use, copy, modify, or distribute the Accenture Tool(s), and (iii) may not reverse assemble, reverse engineer, reverse compile, or otherwise translate such Accenture Tool(s) in any manner except to the extent that applicable law specifically prohibits such restrictions. All such Accenture Tool(s) must be removed at the end of the applicable Incident Investigation, or earlier, if directed by Accenture.

Accenture and its licensors provide the Accenture Tools "as is" and disclaim all express and implied warranties with respect to such Accenture Tools including any implied warranties of merchantability, fitness for purposes or title.

The Accenture data collection tool, to the extent data collection is in scope, includes open source software (OSQuery) and Customer's licenses to such is subject also to the applicable OSS license located at [OSQuery](#).