MASTER SERVICES AGREEMENT

TERMS AND CONDITIONS

This Master Service Agreement ("Agreement") shall apply to the sale of Services from Convercent, Inc. ("Convercent") to its customer ("Customer"), unless Convercent and Customer enter into or have entered into another agreement regarding the Services contemplated herein, and such agreement is in effect as of the Effective Date ("Existing Agreement"), in which case the terms and conditions of the Existing Agreement shall govern the sale of those Convercent Services. Absent an Existing Agreement, this Agreement is effective as of the date an Order Form or Purchase Order is executed ("Effective Date").

1. SERVICES.

1.1 Incorporated Documents. Subject to the terms and conditions of this Agreement and Customer's payment of all applicable fees, Convercent will provide the Services set forth in one or more applicable mutually agreed upon documents (each an **"Order Form")** specifying the subscriptions, licenses, services, or other offerings **("Services")** ordered by Customer under this Agreement. To the extent of any conflict between this Agreement and an Order Form, this Agreement will control, except to the extent the Order Form expressly identifies a provision of the Agreement to be superseded by the Order Form. The attached terms and conditions (including any Exhibits incorporated therein) are hereby all incorporated into this Agreement and are applicable to Customer's purchase of all Services from Convercent.

1.2 Use of the Services. Customer may use the Services ordered by Customer solely for Customer's internal business purposes. Customer may grant administrative access and authority in relation to the Services to employees or contractors of Customer's organization ("**Administrative Users**"), provided that Customer will remain responsible and liable for all actions or omissions of its Administrative Users in connection with the Services. Customer may purchase implementation and configuration Services from Convercent but notwithstanding any such Services, Customer will be solely responsible for; (a) configuring or determining how the Services will be configured for Customer's use; (b) providing for and maintaining any systems, software, hardware, web browser and internet service necessary to access and use the Services; (c) establishing, managing, maintaining, and supporting access rules, incident reporting protocols, authorization of Customer representatives to receive incident reports and communications and any other distribution rules regarding the Services or information contained therein, and (d) providing legally required and appropriate disclosures, and the content thereof, to third parties making reports through the Services. Customer may submit written incident reports online through the Services in English or in another supported language indicated within the Services.

1.3 Restrictions. Customer will not (a) modify, make derivative works of, reverse engineer, disassemble, decompile, or otherwise attempt to discover the source code for the Services; (b) use, evaluate or view the Services for the purpose of designing, modifying, or otherwise creating any environment, program, or infrastructure or any portion thereof, which performs functions similar to the functions performed by the Services; or (c) remove or alter any trademark, logo, copyright, or other proprietary notices, legends, symbols, or labels in the Services.

1.4 Employee Count. Services sold on a subscription-fee basis are priced according to the total number of employees and individual independent contractors of Customer ("**Employee Count**"). Customer represents the initial Employee Count specified on each Order Form is accurate. Additionally, Convercent may request no more than once annually an updated Employee Count from Customer.

For any increase in the Employee Count of greater than five percent (5%), Convercent reserves the right to adjust the pricing ratably for all subscription-fee based Services purchased by Customer hereunder.

1.5 Service Levels.

a. *Web Application*. Convercent will maintain 99.8% uptime of the web-based Services (the "**Web Application SLA**"). The calculation of uptime will exclude scheduled downtime and Force Majeure Events (as defined below). Convercent will inform Customer reasonably in advance of any scheduled downtime.

b. *Call Center*. The call center will be available to receive telephonic reports in the event of an outage within the web application and 80% of calls to the call center will be answered in 20 seconds or less (the "**Call Center SLA**", which, together with the Web Application SLA, the "**SLAs**").

c. *Remedy*. Convercent's sole liability (and Customer's exclusive remedy) for Convercent's breach of either or both SLAs will be to issue a service credit ("**Service Credit**") for the applicable Services for the applicable month, in the amount specified in the table below, which Customer must request by emailing AP@convercent.com within thirty (30) days following the end of the month in which the service level failure occurred. In the event two SLA remedies apply, only the Service Credit for the higher amount will apply.

Actual Web Application Service Level for the month (% of uptime)	Actual Call Center Service Level for the month (% of calls answered in 20 seconds or less)	Service Credit to be issued (% of Customer service fees)
99.0 - 99.79%	75.0 – 79.99%	5%
98.0 – 98.99%	70.0 – 74.99%	10%
95.0 – 97.99%	65.0 – 69.99%	25%
90.0 – 94.99%	60.0 – 64.99%	50%
less than 90%	Less than 60%	100%

1.5 Professional Services. Any professional or advisory Services ordered by Customer hereunder will be provided in accordance with industry standard practices. Any such Services will not constitute legal advice and Customer's use of the Services will not create an attorney client relationship between Customer and Convercent. Customer will not request any legal advice as part of the Services and will consult with independent counsel regarding Customer's use and configuration of the Services.

2. INTELLECTUAL PROPERTY.

2.1 The Services. The Services are licensed, not sold. Convercent and its suppliers exclusively own and retain all rights, title, and interest in and to the Services (including software, user interface designs, and documentation) and all additions and modifications to the Services, including all intellectual property rights therein.

2.2 Customer Data. "**Customer Data**" means all data (including Personal Data as defined below), information, reports, policies, and other content imported to the Services or otherwise provided to

Convercent or its contractors by or for Customer in connection with Customer's use of the Services, and all data and information received by or for Customer from Customer's use of the Services. Customer exclusively owns and retains all rights, title and interest in and to the Customer Data, except for pre-existing Services components contained in such Customer Data (e.g., incident report templates). Customer hereby grants to Convercent and its authorized representatives and contractors a non-exclusive and non-transferable right and license to use, process, store, and transmit, and disclose Customer Data solely to provide the Services to Customer and fulfill other obligations described in this Agreement. Customer further authorizes Convercent to anonymize Customer Data and to aggregate Customer Data with similar data from other Convercent customers in a manner that does not identify Customer or include any Personal Data, to further develop and provide services for Convercent customers.

2.3 **Customer Name and Logo Use**. During the Term, Convercent may include Customer's name and logo in Convercent's standard marketing materials and customer lists provided that Convercent will first obtain Customer's consent for any such use.

3. **FEES AND TAXES**.

3.1 **Fees**. The fees for all Services will be set forth in each Order Form ("**Fees**") and Customer will pay all such Fees in accordance with the terms of this Agreement and the applicable Order Form. Unless otherwise set forth in the applicable Order Form, all Fees due hereunder will be paid annually in advance in U.S. dollars, and will be due within 30 days of the date of the invoice therefor. Should Customer require a PO to purchase, such PO must be issued within 10 days of the Order Effective Date (as defined in the Order Form).

3.2 **Taxes**. Convercent's fees do not include any taxes, levies, duties or similar governmental assessments of any nature (collectively, "**Taxes**"). Customer is responsible for paying all Taxes associated with its purchases hereunder, excluding taxes on Convercent's net income. If Convercent has the legal obligation to pay or collect Taxes for which Customer is responsible under this Agreement, Convercent will invoice Customer and Customer will pay that amount unless Customer provides Convercent a valid tax exemption certificate from the appropriate taxing authority.

4. **TERM AND TERMINATION**.

4.1 **Term**. This Agreement will commence on the Effective Date and, unless earlier terminated in accordance with the Termination for Cause Section, below, will remain in effect so long as any Order Form remains in effect, or, if no such term is specified in an applicable Order Form, for a period of three (3) years (collectively, the "**Term**").

4.2 **Termination for Cause**. Either party may terminate this Agreement upon written notice if the other party is in material breach of this Agreement and such breach remains uncured for thirty (30) days following the breaching party's receipt of written notice of such breach.

4.3 **Effect of Termination**. Upon expiration or termination of this Agreement for any reason: (a) the rights and licenses granted hereunder will cease and the Services will immediately terminate, (b) if requested by Customer, Convercent will, at Customer's cost, make available to Customer (via an SFTP site, for example) the Customer Data held by Convercent (and Customer will assume responsibility for its copy of such Customer Data (and any access thereto) upon download of the Customer Data), and (c) if requested by Customer, Convercent will take reasonable steps to assist with transfer of any dedicated phone numbers used by Convercent or its contractors in connection with the Service. Upon termination by Customer for Convercent's breach, prepaid Fees for Services applicable to the period following termination will be refunded to Customer, less any unpaid Fees for Services. Termination of the Agreement will be without prejudice to either party's rights to seek recovery of damages or pursue any other remedies it may have hereunder or under applicable law. The Restrictions, Intellectual Property, Fees and Taxes, and Effect of Termination Sections, as well as all Sections from and including Confidentiality through General Provisions, will survive the expiration or termination of this Agreement for any reason.

5. **CONFIDENTIALITY.** Each party acknowledges that the Confidential Information (as hereinafter defined) of the other party may contain information valuable to the Disclosing Party, and each party that receives such Confidential Information (the "**Receiving Party**") from the other party (the "**Disclosing Party**") agrees that Confidential Information will remain the property of the Disclosing Party. Receiving Party will not make use of Disclosing Party's Confidential Information, except as authorized by this Agreement and to the extent necessary for performance or enforcement of this Agreement; and Receiving Party will keep Disclosing Party's Confidential Information confidential and not disclose to any third party, except to such Receiving Party's employees and contractors who need to know such information in order for such party to perform this Agreement and only to the extent they are bound by confidentiality and non-use obligations not less restrictive than this Agreement. If Customer provides any feedback, comments, or ideas to Convercent regarding the Services or improvements thereto, Customer agrees that Convercent will be free to use, disclose, and exercise any rights in the same in connection with its products and services. "**Confidential Information**" means all information that is, or should be reasonably understood to be, confidential or proprietary information of the Disclosing Party (and its suppliers, contractors and customers), including without limitation information concerning its business, products, services, finances, employees, contractors, software, notes, documentation, tools, processes, protocols, product designs and plans, customer lists and other marketing and technical information; and the terms of this Agreement, whether disclosed orally or in writing by any other media. Confidential Information includes all software and related user documentation included in the Services, Customer Data, and excludes information that (a) is or becomes generally known to the public through no fault or breach of this Agreement by the Receiving Party; (b) is independently developed by a party without reference to the Confidential Information of the other party; (c) was in the Receiving Party's possession free of any obligation of confidence at the time it was communicated to the Receiving Party; or (d) is rightfully obtained by a party from a third party without restriction on use or disclosure. Notwithstanding the foregoing, the Receiving Party will not be in violation of this Section with regard to disclosure of Confidential Information in response to an order or subpoena of a court, agency or tribunal of competent jurisdiction, or pursuant to any applicable law or regulation, provided that the Receiving Party provides the Disclosing Party with prior written notice of such disclosure to the extent reasonably practicable and legally permissible in order to permit the Disclosing Party to seek confidential treatment of such information.

6. **REPRESENTATIONS AND WARRANTIES; DISCLAIMER**.

6.1 Warranties. Each party represents and warrants to the other party that (a) it has and will have full right and authority to enter into this Agreement and to grant the rights provided hereunder, (b) this Agreement will be enforceable against it, and (c) the entry into and performance of this Agreement by it do not contravene other agreements, laws, or orders to which it is subject. Customer represents and warrants that Customer will not make or publish any representations, warranties, or guarantees to any users of the Services.

6.2 Disclaimer. EXCEPT AS EXPRESSLY PROVIDED IN THIS REPRESENTATIONS AND WARRANTIES; DISCLAIMER SECTION, NEITHER PARTY MAKES ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND AND EACH PARTY SPECIFICALLY DISCLAIMS ALL OTHER REPRESENTATIONS, WARRANTIES, AND CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. WITHOUT LIMITING THE FOREGOING, CONVERCENT DOES NOT REPRESENT OR WARRANT THAT THE SERVICES WILL MEET ALL OF CUSTOMER'S REQUIREMENTS OR BE UNINTERRUPTED, SECURE,

COMPLETE, ERROR-FREE, OR FREE OF VIRUSES, MALICIOUS CODE, OR OTHER HARMFUL COMPONENTS, OR THAT ALL DEFECTS WILL BE CORRECTED.

7. INDEMNIFICATION.

7.1 By Convercent. Convercent will indemnify, defend, and hold harmless Customer from and against any third-party suit and the damages finally awarded therein ("**Claim**") which alleges that the Services infringe, misappropriate or violate the intellectual property right of any third party.

7.2 By Customer. Customer will indemnify, defend, and hold harmless Convercent from and against any and all Claims which allege that any Customer Data infringes, misappropriates or violates the intellectual property right of any third party or relate to or are based on incident reports submitted to Customer via the Services.

7.3 Indemnification Procedure. Each party's indemnification obligation above is subject in each instance to the indemnified party (i) promptly giving notice of the Claim to the indemnifying party; (ii) giving the indemnifying party sole control of the defense and settlement of the Claim (provided that the indemnified party will have the right to approve any material liability imposed on and borne by the indemnified party in connection with such settlement); and (iii) providing to the indemnifying party all available information and reasonable assistance.

7.4 Exceptions. Notwithstanding the foregoing, Convercent will not have any indemnification obligations pursuant to this Agreement to the extent any Claim arises from (i) use of the Services outside the scope of the rights granted to Customer in this Agreement; (ii) use of the Services with other products, software or materials not furnished by Convercent where the Services would not themselves be infringing; or (iii) the modification or improvement of the Services by Customer or any third party; or (iv) any continued use by Customer of an allegedly infringing item or continued allegedly infringing activity by Customer after Convercent has replaced or modified the item or instructed Customer to modify the activity so that it becomes non-infringing.

7.5 Replacement or Modification. Should the use of any Services or portion thereof be enjoined or threatened to be enjoined or determined to be infringing any third party intellectual property right, Convercent will notify Customer and, at Convercent's expense Convercent may: (a) procure for Customer the right to continue use of the Services as contemplated under this Agreement, (b) replace or modify the Services to be non-infringing, or (c) if "(a)" or "(b)" are not economically feasible for Convercent, then Convercent will have the right to terminate the obligations with regards to such Services.

8. Limitation of Liability. EXCEPT FOR BREACHES OF THE CONFIDENTIALITY SECTION, NEITHER PARTY WILL BE LIABLE TO THE OTHER FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, FINES OR PENALTIES, COSTS OF PROCUREMENT OF SUBSTITUTE SERVICES OR TECHNOLOGY, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS, OR FOR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, REGARDLESS OF THE LEGAL OR EQUITABLE THEORY ON THE BASIS OF WHICH ANY CLAIM FOR DAMAGES IS BROUGHT, INCLUDING, BUT NOT LIMITED TO, BREACH OF CONTRACT, TORT OR STATUTE, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXCEPT WITH RESPECT TO BREACHES OF THE CONFIDENTIALITY SECTION, OBLIGATIONS PROVIDED IN THE INDEMNIFICATION SECTION, AND CUSTOMER'S PAYMENT OBLIGATIONS UNDER THE APPLICABLE ORDER FORM, IN NO EVENT WILL EITHER PARTY'S LIABILITY TO THE OTHER UNDER OR IN RESPECT OF THIS AGREEMENT EXCEED THE EQUIVALENT OF TWELVE (12) MONTHS OF FEES PAID OR PAYABLE FOR SERVICES DURING THE TWELVE (12) MONTH PERIOD PRECEDING THE LIABILITY.

9. Compliance with Law. In performing its obligations or exercising its rights under this Agreement, each party will comply with all applicable laws and government regulations at all times, including but not limited to any applicable laws and regulations of the United States and other jurisdictions relating to export or re-export of technology, consumer protection, information access and privacy.

10. DATA PROTECTION.

10.1 Personal Data. In the course of performing the Services for Customer, Convercent may receive and store information that can be used to uniquely identify, contact or locate a natural person, including but not limited to name, address, email address, or phone number ("**Personal Data**"). Convercent will safeguard the confidentiality of Personal Data in accordance with Exhibit A and will not access or use such Personal Data other than as necessary to perform the Services. Convercent receives and stores Personal Data solely as an agent acting on behalf of Customer.

10.2 Security. The Convercent product and applications are ISO 27001:2013 and HITRUST CSF certified and Convercent will protect all Customer Data as described in Exhibit A. At Customer's request, Convercent will provide to Customer third party assessments and compliance certifications it makes available to all customers, including an annual Service Organization Controls (SOC) 2 Type II report ("**SOC 2 Report**") as defined by the American Institute of Certified Public Accountants. Such SOC 2 Report will include an opinion by the independent auditor on the adequacy and integrity of Convercent's general controls for security.

10.3 EU Law. If the parties agree that the Services will involve the processing by Convercent of Personal Data from the European Union, then Convercent will perform all such processing in compliance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and the Data Processing Addendum that the parties will attach hereto as Exhibit B.

11. GENERAL PROVISIONS.

11.1 Independent Contractors. The parties are independent contractors, and no agency, partnership, franchise, joint venture, or employment relationship is intended or created by this Agreement.

11.2 Severability. If any provision herein is held to be invalid or unenforceable for any reason, the remaining provisions will continue in full force and effect without being impaired or invalidated in any way. The parties agree to replace any invalid provision with a valid provision that most closely approximates the intent and economic effect of the invalid provision.

11.3 Waiver. Neither party will be deemed to have waived any provision hereof unless such waiver is in writing and executed by a duly authorized officer of both parties. Except as otherwise set forth in this Agreement, no failure to exercise or delay in exercising any rights arising from this Agreement will operate or be construed as a waiver thereof.

11.4 Force Majeure. With the exception of any monetary obligations under this Agreement, neither party will be responsible for performance of its obligations hereunder where delayed or hindered by events beyond its reasonable control, including, without limitation, acts of God or any governmental body, war or national emergency, riots or insurrection, sabotage, embargo, fire, flood, accident, strike or other labor disturbance, or interruption of or delay in systems, power or telecommunications under third-party control ("**Force Majeure Events**").

11.5 Notice. To be effective, any notice required to be given under this Agreement will be given in writing, addressed to the applicable party (at the address in the Order Form) and hand delivered, which is effective upon delivery; sent by reputable overnight courier, which is effective on the business day following deposit with such courier; or sent by the United States mail, first class postage prepaid, which is effective on the third business day after deposit in the United States mail.

11.6 **Governing Law and Venue**. This Agreement will be governed and construed in accordance with the laws of the State of Delaware without giving effect to any principles that may provide for the application of the law of any other jurisdiction. Any legal suit, action or proceeding arising out of or related to this Agreement or the matters contemplated hereunder will be instituted exclusively in the federal courts of the United States or the courts of the State of Delaware, in each case located in the State of Delaware (except where such courts do not have jurisdiction), and each party irrevocably submits to the exclusive jurisdiction of such courts in any such suit, action or proceeding and waives any objection based on improper venue or forum non conveniens. In the event of litigation arising out of this Agreement, the prevailing party will be entitled to its costs and reasonable attorneys' fees.

11.7 **Assignment**. Neither party may assign this Agreement or any right, interest or benefit under this Agreement without the prior written consent of the other party; provided, however, either party may assign this Agreement to a successor who acquires substantially all of the assets or equity of such party through purchase, merger or other transaction without the other party's consent. Any purported assignment in breach of the foregoing will be null and void. This Agreement will be fully binding upon, inure to the benefit of and be enforceable by the parties hereto and their respective successors and permitted assigns, and nothing in this Agreement confers upon any other person or entity any legal or equitable right whatsoever to enforce any provision of this Agreement.

11.8 **Entire Agreement**. This Agreement (together with any Order Forms) constitutes the entire agreement between the parties concerning the subject matter hereof and supersedes all prior and contemporaneous agreements and communications, whether oral or written, between the parties relating to the subject matter hereof, and all past courses of dealing or industry custom. No modification, amendment, or waiver of any provision of this Agreement will be effective unless in a writing duly executed by authorized representatives of both parties. Any standard terms associated with a Customer purchase order or other order document (e.g., general terms and conditions attached to the purchase order form) will be not binding on the parties and of no consequence whatsoever in interpreting the parties' legal rights and responsibilities as they pertain to Services provided under this Agreement. Similarly, any terms required to be accepted electronically through any Customer vendor enrollment, login, invoice submission, or other, process will not apply to this Agreement, are expressly rejected by the parties, and form no basis for any agreement between the parties; notwithstanding any indication of "agreement" to such terms, no such agreement is formed between the parties and the parties acknowledge that only authorized representatives of the parties may enter into agreements between the parties or amendments to this Agreement.

Exhibit A

Data Security

1. PURPOSE AND SCOPE.

This Data Security Exhibit (this **"Exhibit"**) describes data protection and information security standards that Convercent maintains in order to protect Customer Data from unauthorized use, access, disclosure, theft, manipulation, or reproduction. Capitalized terms used but not defined in this Exhibit will have the meaning set forth in the Agreement.

2. DEFINITIONS.

a. "**Applicable Laws and Regulations**" mean any data protection, privacy or information security laws, codes and regulations or other binding restrictions governing Processing of Customer Data, including Personal Data, that are applicable to Convercent's Processing of Customer Data under the Agreement.

b. "**Breach**" or "**Security Breach**" means a compromise (including but not limited to misuse, loss, destruction, or unauthorized access, collection, retention, storage, or transfer) of the systems in which Customer Data has been accessed or acquired by one or more unauthorized parties or any act that violates any Applicable Laws and Regulations.

c. "**Data Center**" means a location at which Convercent Processes Personal Data under this Agreement. Data Centers can be Convercent-owned or third-party service model-based.

d. **"Industry Standard Encryption Algorithms and Key Strengths"** means encryption will at least meet the following standard encryption algorithm (note: The algorithm and key strengths may change depending upon the new and most up-to-date industry standard encryption practice):

- Symmetric encryption: AES (≥ 128-bit);
- Asymmetric encryption: RSA (≥ 2048-bit);
- Hashing: SHA-2 (≥ 224-bit) with "salt" will be added to the input string prior to encoding to ensure that the same password text chosen by different users will yield different encodings.

e. "**Processing**", "**Processes**" or "**Process**" means any operation or set of operations which is performed upon Customer Data, whether by automatic means or not, including but not limited to collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

3. SECURITY MANAGEMENT.

3.1 <u>**Scope and Contents**</u>. Convercent will develop, implement, maintain and enforce a written information privacy and security program ("**Security Program**") that (i) complies with ISO 27001 and HITRUST CFS, (ii) includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity and availability of Customer Data and (iii) is appropriate to the nature, size and complexity of Convercent's business operations; and (iv) complies with any Applicable Laws and Regulations.

a. <u>Security Program Changes</u>. Convercent will provide details of any major changes to its Security Program that may adversely affect the security of any Customer Data.

b. Security Officer. Convercent will designate a senior employee to be responsible for overseeing and carrying out its Security Program and for communicating with Customer on information security matters ("**Convercent's Security Officer**"). Upon Customer's request, Convercent's Security Officer will provide Customer with the contact information of one or more Convercent representatives who will be available to discuss any security concerns (e.g., discovered vulnerability, exposed risk, reported concern) with Customer and to communicate the level of risk associated with such concerns and any remediation thereof.

3.2 Personnel Security.

a. Verification Checks. Prior to assigning any of its Personnel to positions in which they will, or Convercent reasonably expects them to, have access to Customer Data, Convercent will conduct or verify background checks on such Personnel, except where expressly prohibited by law. For the purposes of this Exhibit, "**Personnel**" means Convercent's employees, independent contractors, and subcontractors that have access to Personal Data.

b. Training. Convercent Personnel will, upon hiring, and at least annually thereafter, participate in security awareness training. This training will cover, at a minimum, Convercent's security policies, including acceptable use, password protection, data classification, Breach reporting, the repercussions of violations, and brief overviews of Applicable Laws and Regulations.

c. Due Diligence over Subcontractors. Convercent maintains a security process to conduct appropriate due diligence prior to utilizing subcontractors to provide any of the Services. Convercent will assess the security capabilities of any such subcontractors on an annual basis to ensure subcontractor's ability to comply with this Exhibit and the terms of the Agreement. The due diligence process will provide for the identification and resolution of significant security issues prior to engaging a subcontractor, written information security requirements that require subcontractor to adhere to Convercent's key information security policies and standards within all contracts, and for the identification and resolution of any security issues during the term of the Agreement.

4. PHYSICAL SECURITY.

4.1 General. The physical security processes in this Section apply to all facilities used to provide the Services at which Customer Data is accessed, processed, stored, transferred or maintained, including any floor space where Services are performed in which Personnel have access to Customer Data and servers or other equipment that processes or stores Customer Data (the "**Secure Area**").

4.2 Secure Area. Customer Data will only reside within a Secure Area. Convercent will restrict access to and will control and monitor all physical areas in Convercent's premises that contain Customer Data. Convercent will secure and monitor access to any Secure Area and will maintain physical security controls at the Secure Area, on a 24-hours-per-day, 7-days-per-week basis ("**24/7**"). Convercent will revoke any Personnel's access to Secure Areas within twenty-four (24) hours of the cessation of such Convercent Personnel's need to access buildings, system(s) or application(s).

4.3 Data Centers. To the extent Convercent is operating a Data Center or utilizing a Third-Party Data Center, Convercent will comply with physical security controls outlined in industry standards such as ISO 27001, SSAE 16 or ISAE 3402, or PCI-DSS. All access to areas, cabinets, or racks that house telecommunications, networking devices and other "data transmission lines" or equipment will be controlled as follows:

a. access will be controlled by badge reader at one or more entrance points;

b. doors used only as exit points will have only "one way" doorknobs or crash bar exit devices installed;

c. all doors will be equipped with door alarms contacts;

d. all exit doors will have video surveillance capability; and

e. all card access and video surveillance systems will be tied into generator or UPS backup systems.

5. LOGICAL SECURITY.

5.1 **General**. The logical security processes in this Section apply to all Convercent's systems or Convercent's agents' or its assigns' systems and supporting networks used to provide the Services on which Customer Data is accessed, processed, stored, transferred or maintained.

5.2 **Systems Access Control and Network Access Control**.

a. Access Controls. Convercent employs access control mechanisms that:

   i. prevent unauthorized access to Customer Data;

   ii. limit access to Personnel with a business need to know;

   iii. follow principle of least privilege allowing access to only the information and resources that are necessary under the terms of the Agreement; and

   iv. have the capability of detecting, logging, and reporting access to the system or network or attempts to breach security of the system or network.

b. Accounts. All Personnel must have an individual account that authenticates that individual's access to Customer Data. Convercent does not allow sharing of accounts. Access controls and passwords are configured in accordance with industry standards and best practices. Passwords will be hashed with industry standard algorithms per the Storage, Handling and Disposal Section, below.

c. Regular Review of Access Controls. Convercent maintains a process to review access controls on a minimum annual basis for all Convercent systems that contain Customer Data, including any system that, via any form of communication interface, can connect to the system on which Customer Data is stored. These access processes and the process to establish and delete individual accounts will be documented in, and will be in compliance with, Convercent's security policies and standards referenced in the Security Management: Scope and Contents Sub-section, above. Convercent maintains the same processes of review and validation for any third party hosted systems it uses that contain Customer Data.

d. Remote Access Authentication. Convercent will configure remote access to all networks storing or transmitting Customer Data to require two-factor authentication for such access or at a minimum will use access control lists to only allow connectivity to such networks from Convercent's own network.

e. Revocation of Access. Convercent will revoke Personnel's access to physical locations, systems, and applications that contain or process Customer Data within twenty-four (24) hours of the cessation of such Personnel's need to access the system(s) or application(s).

5.3 **Telecommunication and Network Security**.

a. Convercent will deploy reasonably appropriate firewall technology in the operation of Convercent's sites. Traffic between Customer and Convercent will be protected and authenticated by industry standard cryptographic technologies. Specifically, firewall(s) must be able to effectively perform the following functions: stateful inspection, logging, support for all IPSec standards and certificates, support for strong encryption and hashing, ICMP and SNMP based monitoring and anti-spoofing.

b. Firewall Maintenance. At a minimum, Convercent will review firewall rule sets annually to ensure that legacy rules are removed and active rules are configured correctly.

c. Intrusion Detection and Prevention. Convercent will deploy intrusion detection or preferably prevention systems (NIDS/NIPS) in order to generate, monitor, and respond to alerts which could indicate potential compromise of the network and/or host.

d. Log Management. Convercent will deploy a log management solution and retain logs produced by firewalls and intrusion detection systems for a minimum period of one (1) year.

e. Network Segmentation. Convercent will establish and maintain appropriate network segmentation, including the use of virtual local area networks (VLANS) where appropriate, to restrict network access to systems storing Customer Data. Convercent will proxy all connections from public networks into Convercent's internal network using DMZ or equivalent. Convercent will not allow direct connections from public networks into any network segment storing Customer Data.

5.4 Malicious Code Protection.

a. All workstations and servers will run the current version of industry standard anti-virus software with the most recent updates available on each workstation or server. Virus definitions must be updated within twenty-four (24) hours of release by the anti-virus software vendor. Convercent will configure this equipment and have supporting policies to prohibit users from disabling anti-virus software, altering security configurations, or disabling other protective measures put in place to ensure the safety of Customer's or Convercent's computing environment.

b. Convercent will have current anti-virus software configured to run real-time scanning of machines and a full system scan on a regularly scheduled interval not to exceed seven (7) calendar days.

c. Convercent will scan incoming and outgoing content for malicious code on all gateways to public networks, including, but not limited to, email and proxy servers.

d. Convercent will quarantine or remove files that have been identified as infected and will log the event.

5.5 Data Loss Prevention. Convercent will employ a system to prevent the inadvertent or intentional compromise of Customer Data. Controls must exist to track activity, inspect network traffic, including email and other protocols, and filter/block certain user actions to ensure Customer Data remains secured.

6. SYSTEMS DEVELOPMENT AND MAINTENANCE.

6.1 **Documentation**. Convercent will maintain documentation on overall system, network, and application architecture, data flows, process flows, and security functionality for all applications that process or store any Customer Data.

6.2 **Change Management**. Convercent will employ an effective, documented change management program with respect to the Services as an integral part of its security profile. This includes logically or physically separate environments from production for all development and testing. No Customer Data will be transmitted, stored or processed in an environment that does not maintain at least the minimum administrative, technical and physical safeguards as described in this Exhibit.

6.3 **Vulnerability Management and Application Security Assessments**. Convercent will run internal and external network vulnerability scans at least quarterly and after any material change in the network configuration (e.g., new system component installations, changes in network topology, firewall rule modifications, or product upgrades). Vulnerabilities identified and rated as high risk by Convercent will be remediated within ninety (90) days of discovery.

1. For all Internet-facing applications that collect, transmit or display Customer Data, Convercent agrees to conduct an application security assessment review to identify common security vulnerabilities as identified by industry-recognized organizations (e.g., OWASP Top 10 Vulnerabilities; CWE/SANS Top 25 vulnerabilities) annually or for all major releases, whichever occurs first. The scope of the security assessment will primarily focus on application security, including, but not limited to, a static code analysis or penetration test of the application, as well as a code review. At a minimum, it will cover the OWASP Top 10 vulnerabilities (https://www.owasp.org).

2. Convercent may utilize a qualified third party to conduct the application security assessments. Convercent may conduct the security assessment review themselves, provided that Convercent's Personnel performing the review are sufficiently trained, follow industry standard best practices, and the assessment process is reviewed and approved by Customer. Vulnerabilities identified and rated as high risk by Convercent will be remediated within ninety (90) days of discovery.

6.4 **Source code review**. Convercent will have a documented program for secure code reviews and maintain documentation of secure code reviews performed for all applications that store or process Customer Data.

6.5 **Patch Management**. Convercent will patch all workstations and servers with all current operating system, database and application patches deployed in Convercent's computing environment according to a schedule predicated on the criticality of the patch. Convercent will perform appropriate steps to help ensure patches do not compromise the security of the information resources being patched. All emergency or critical rated patches must be applied as soon as possible but at no time will exceed six weeks from the date of release.

7. **Email Security**. If Convercent is sending emails to Customer customers or employees, appropriate email identity solutions, including but not limited to DKIM, SPF, and DMARC, will be utilized.

8. **CUSTOMER SECURITY ASSESSMENTS AND AUDITS**.

8.1 Convercent agrees, upon written request no more than on an annual basis, to allow its procedures and documentation to be inspected by Customer (or its designee) in order to ascertain compliance with Applicable Laws and Regulations, this Exhibit, or any non-disclosure agreements and any agreements between Customer and Convercent.

8.2 Convercent will reasonably cooperate with audit requests by providing access to relevant knowledgeable personnel, documentation, and application software.

9. Breach Notification and Response Procedures.

9.1 Notification. Convercent will maintain an incident response function capable of identifying, mitigating the effects of, and preventing the recurrence of, Security Breaches. Upon discovering or otherwise becoming aware a Breach, Convercent will take all reasonable measures to mitigate the harmful effects of the Breach. Convercent will also notify Customer of the Breach as soon as practicable, but in no event later than 48 hours after the Breach. Notice to Customer will include: (i) the identification of the Customer Data which has been or Convercent reasonably believes has been used, accessed, acquired or disclosed during the incident; (ii) a description of what happened, including the date of the incident and the date of discovery of the incident, if known; (iii) the scope of the incident, including a description of the type of Customer Data involved in the incident; (iv) a description of Convercent's response to the incident, including steps Convercent has taken to mitigate the harm caused by the incident; and (v) other information as Customer may reasonably request and is reasonably applicable. Convercent agrees to cover the costs of any such notification, including reimbursing Customer for any reasonable costs.

9.2 Response. Convercent will retain all data related to known and reported Breaches or investigations until Convercent reasonably determines that the data is no longer needed. Upon Customer's request, Convercent will permit Customer or its third-party auditor to review and verify relevant video surveillance records, access logs and data pertaining to any Breach investigation. Upon conclusion of investigative, corrective, and remedial actions with respect to a Breach, Convercent will prepare and deliver to Customer a final report that describes in detail: (i) the extent of the Breach; (ii) the Customer Data disclosed, destroyed, or otherwise compromised or altered; (iii) all supporting evidence, including, but not limited to, system, network, and application logs; (iv) all corrective and remedial actions completed; and (v) all efforts taken to mitigate the risks of further Breaches.

10. Storage, Handling and Disposal.

10.1 Data Segregation. Convercent will physically or logically separate and segregate Customer Data from its other clients' data.

10.2 Electronic Form Data. Convercent will utilize Industry Standard Encryption Algorithms and Key Strengths (as defined in the Definitions Section of this Exhibit) to encrypt the following:

a. All Customer Data that is in electronic form while in transit over all public wired networks (e.g., Internet) and all wireless networks;

b. All Customer Data stored in databases, in file systems, and on various forms of online and offline media (DASD, tape, etc.);

c. Passwords for privileged access will be hashed with irreversible industry standard algorithms with randomly generated "salt" added to the input string prior to encoding to ensure that the same password text chosen by different users will yield different encodings. The randomly generated salt will be at least as long as the output of the hash function; and

10.3 Key Management. Where encryption is utilized, Convercent will maintain a key management process that meets the following minimum requirements:

1. At least one key custodian must be officially designated.
2. Key custodians must ensure that all keys used in a storage encryption solution are secured and managed properly to support the security of the solution.
3. Key management must be planned to include secure key generation, use, storage and revocation.

4. Key management practices must support the recovery of encrypted data if a key is inadvertently disclosed, destroyed or becomes unavailable.

5. Key custodians must ensure that access to encryption keys is properly restricted to approved administrators. Private keys must not be stored on the same media and/or virtual instance as the data they protect.

6. Authentication must be required in order to gain access to keys.

7. Keys will be rotated annually and must be replaced before they expire.

10.4 **Physical Form Data**. Convercent will only store Customer Data in physical form in a Secure Area, and Convercent will establish and operate a document control system to record and track the transfer of all Customer Data that is in physical form both (i) between and within Convercent facilities, and (ii) via any external shipment. Such a control system will include, at minimum, a description of the specific records being transferred (e.g., customer or employee records, etc.), as well as the parties who are preparing, shipping, receiving, and processing such materials.

10.5 **Shipments**. Convercent will transfer all Customer Data in physical form (i.e. external hard drives, backup tapes, etc.) in secure containers or packaging. Convercent will ship any Customer Data in physical form via controlled transportation methods reasonably designed to prevent unauthorized access or compromise, including encryption of electronic media where applicable. Controlled transportation methods include enclosed locked vehicles, registered mail, and commercial shipping services with numbered tracking capability (e.g., UPS, FedEx).

10.6 **Data Retention**. Except where prohibited by law, upon (i) the date of expiration or termination of the Agreement; (ii) when Customer Data is no longer required for the purposes of the Agreement; or (iii) at any time upon written request from Customer, whichever occurs earliest:

a. Convercent will promptly remove the Customer Data from Convercent's database and destroy it within a reasonable timeframe, but in no case longer than thirty (30) days thereafter; and

b. Convercent will provide Customer with a written certification regarding such removal and destruction upon request.

11. BUSINESS CONTINUITY AND DISASTER RECOVERY.

Convercent will set up a Business Continuity Management program that meets the needs of the business and Services being provided to Customer. To that end, a minimum level of crisis management, business continuity, and disaster recovery planning will be completed by Convercent.

a. Business Continuity, and Disaster Recovery Plans will be as follows:

- A Business Continuity Plan includes, but is not limited to, elements such as event management, life safety, business recovery, alternative site locations, and call tree testing.

- A Disaster Recovery Plan includes, but is not limited to, infrastructure, technology, and system(s) details, recovery activities, and identifies the people / teams required for such recovery.

b. Plan Content. The Business Continuity Plan and Disaster Recovery Plan will address actions that Convercent will take in the event of an extended outage of Service and will include test results for the Business Continuity and Disaster Recovery Plan from a test performed annually. Convercent will ensure that its plans address the actions and resources required to provide for (i) the continuous operation of Convercent, and (ii) in the event of an interruption, the recovery of the functions required to enable Convercent to provide the Services described in the Agreement, including all required systems, hardware, software, resources, personnel and data supporting these functions, within a time period time sufficient to meet service levels described in the Agreement.

12. **Survival**. Convercent's obligations and Customer's rights under this Exhibit will become effective on the Effective Date of the Agreement and will continue in effect so long as Convercent possesses Customer Data.

13. **Conflict**. If and to the extent language in this Exhibit or any of its Schedule conflicts with the Agreement, this Exhibit will control.

Exhibit B

Data Processing Addendum

(To be attached as needed)