Converge Technology Solutions Corp. (“Converge”)

End User License Agreement (EULA)

Services: Converge Enterprise Cloud for IBM Guardium Insights (CECIGI) (defined as “Services”)

Dated: March 23, 2022

INTRODUCTION

This EULA governs your use of the Services; by using the Services, you accept these terms and conditions in full. If you disagree with these terms and conditions or any part of these terms and conditions, you must not use the Services purchased hereunder.

By accepting this EULA, you also accept the Data Processing Agreement found here: https://convergetp.com/wp-content/uploads/2022/04/DPA-Converge-Enterprise-Cloud-for-IBM-Guardium-Inisghts-CECIGI.pdf

DESCRIPTION OF SERVICES

Converge will provide you a cloud-based IBM Security Guardium Insights (“Guardium Insights”) environment that is fully hosted, managed, and maintained by Converge. Converge will deploy the environment on Converge’s cloud platform with proactive health monitoring and remediation of all layers of the Guardium Insights environment as well as regular patching and maintenance.

Additionally, Converge will provide the following Services:

- Gather details around your existing IBM Security Guardium Data Protection (“Guardium Data Protection") environment, when applicable
- Instantiate your Guardium Insights cluster
- Build up to three (3) Guardium Insights reports for your consumption
- Work with your IBM Guardium administrators to enable the data flow from your Guardium Data Protection environment to your hosted Guardium Insights environment

- Work with your system administrator(s) to enable user authentication to your Guardium Insights environment via LDAP
- Provide instruction to you on how to access and navigate the environment
- Ensure your Guardium Insights environment is functioning correctly and accessible on a 24/7 basis during the Services term

Converge will deploy your IBM Security Guardium Insights environment in one of three major cloud providers selected by you:

- Amazon Web Services ("AWS")
- Google Cloud Platform ("GCP")
- Microsoft Azure ("Azure")

Converge will be provided the following information by you or your reseller which are necessary to start the Services:

- Your IBM Customer Number
- Your IBM Site ID
- Details of the quantities of Services you purchased from IBM
- Your preferred cloud provider (AWS, Azure, or Google Cloud) for hosting the environment
- A primary contact name and email address of someone in your organization for the purposed of coordinating deployment of the Services

Converge sells the Services using a Resource Unit (RU) metric for the Converge Enterprise Cloud for IBM Guardium Insights Capacity part, which is sold in bundles of 100 RUs. The amount of entitlement required of the Service based on the number of Managed Virtual Servers (MVS) and/or Virtual Processor Cores (VPC) in your environment. MVSs and VPCs are converted to RUs using the following formulas:

- 1 Managed Virtual Server (MVS) : 100 RUs
- 1 Virtual Processor Core (VPC) : 10 RUs

SUPPORTED IBM SECURITY GUARDIUM DATA SOURCES

Converge will work with you to connect your IBM Guardium Data Protection environment to your hosted Guardium Insights environment provided the data sources are supported by IBM on the delivery date and will remain supported through the duration of the Services Term. Data sources are defined as follows:

- Guardium Data Protection Central Manager appliances
- Guardium Data Protection Aggregator appliances
- Guardium Data Protection Collector appliances
- Publicly Available Guardium Universal Connectors
- Guardium External S-TAPs

SERVICES REGION

The region in which the Services will be performed is limited to the United States of America.

IBM SECURITY GUARDIUM INSIGHTS SOFTWARE VERSION

Converge will use the latest available major version of the IBM Guardium Insights software when instantiating your Guardium Insights cluster provided the major version has been fully vetted by Converge. Additionally, Converge will update the software version when minor updates are generally available provided that the minor version that has been fully vetted by Converge. Software vetting will be conducted within a commercially reasonable timeframe after IBM's release of that software version.

PRODUCTS EMBEDDED IN THE SERVICES

Any products embedded as part of the Services shall be governed by the Original Equipment Manufacturer ("OEM") terms and conditions. You shall accept any OEM terms and conditions and you shall accept such terms and conditions, or you will be denied access to the Services.

LICENSE TO USE THE SERVICES

Unless otherwise stated, Converge and/or its licensors own the intellectual property rights in the Services. Subject to the license below, all these intellectual property rights are reserved.

- You must not use the Services in any way that causes, or may cause, damage or impairment of the availability or accessibility of the Services; or in any way which is unlawful, illegal, fraudulent or harmful, obscene, offensive, or in connection with any unlawful, illegal, fraudulent or harmful purpose or activity.
- You must not use the Services to copy, store, host, transmit, send, use, publish or distribute any material which consists of (or is linked to) any spyware, computer virus, Trojan horse, worm, keystroke logger, rootkit or other malicious computer software.

- You must not conduct any systematic or automated data collection activities (including without limitation scraping, data mining, data extraction and data harvesting) on or in relation to the Services without Converge's express written consent.
- You must not use the Services to transmit or send unsolicited commercial communications.
- You must not use the Services for any purposes related to marketing without Converge's express written consent.
- The full *Acceptable Use Policy* is attached as Exhibit A.

TERM AND TERMINATION

- Converge agrees to provide you Services for minimum 12-month service term which begins on the date Converge notifies you that you can access the Services ("Delivery Date").
- The Services term will automatically renew on the anniversary of the Delivery Date for an additional 12-month term provided you are entitled to us Guardium Insights. You must provide proof your IBM Security Guardium Insights software and Services entitlements upon Services renewal to be in compliance with your IBM Software and Support Agreement.
- For automatic renewal, unless you provide written notice of non-renewal to Converge at least 30 days prior to the term expiration date, the Services will automatically renew for the specified term.

TERMINATION OF SERVICES

- You may terminate the Services on thirty days' notice:
    (1) At the written recommendation of a government or regulatory agency following a change in either applicable law or the Services;
    (2) If a change to the Services causes you to be noncompliant with applicable laws; or
    (3) If Converge notifies you of a change to the Services that has a material adverse effect on your use of the Services; provided that Converge will have 90 days to work with you to minimize such effect.
- You may terminate the Services for material breach of Converge's obligations if all requirements below are met:
    - You provide a written complaint to Converge detailing how the Services do not meet its written specification.

    - You and Converge will work together in good faith to investigate and assess the compliant. If Converge determines your compliant to be valid, Converge will attempt to resolve the issue in a commercially reasonable amount of time.
    - If the issue can't be resolved in a commercially reasonable amount of time, and you decide to terminate services Converge will terminate services. You will still owe any payments for services delivered in the term.
- Upon termination, Converge may assist you in transitioning your content to an alternative technology for an additional charge and under separate agreement terms.
- Upon termination, your access to the hosted Guardium Insights environment will be revoked and Converge will notify you of the revocation via email. The notification will include details on when the hosted Guardium Insights environment will be decommissioned. Following decommissioning, you'll receive a notice that the data contained within your hosted Guardium Insights environment has been deleted. **USE OF CONTENT**
- Converge and its affiliates will access and use your content solely for the purpose of providing and managing the Services.
- Converge will treat your content as confidential by only disclosing to Converge employees to the extent necessary to provide the Services.

SUSPENSION OF SERVICE

- Converge may suspend or limit, to the extent necessary, your use of the Service if Converge reasonably determines there is a:
    (1) material breach of your obligations;
    (2) security breach;
    (3) violation of law; or
    (4) breach of the terms and conditions
- Converge will provide notice prior to a suspension as commercially reasonable.
- If the cause of suspension can reasonably be remedied, Converge will provide notice of the actions you must take to reinstate the Services. If you fail to take such actions with a reasonable time, Converge may terminate the Services.

WARRANTIES

- Converge warrants that it provides the Services using commercially reasonable care and skill.
- The warranties end when the Services end.
- These warranties are the exclusive warranties from Converge and replace all other warranties, including the implied warranties or conditions of satisfactory quality, merchantability, non-infringement, and fitness for a particular purpose.

WARRANTY LIMITATION

- Converge does not warrant uninterrupted or error-free operation of the Services.
- Converge does not warrant it will correct all defects.
- While Converge endeavors to provide security measures to keep all data secure, Converge does not warrant Converge can prevent all third-party disruptions or unauthorized third-party access.
- Converge warranties will not apply if there has been misuse, modification, damage not caused by Converge, or failure to comply with written instructions provided by Converge.

CUSTOMER RESPONSIBLITIES

You are solely responsible for (i) obtaining all necessary rights and permissions to permit processing of your content in the Services (ii) you will make disclosures and obtain consent required by law before you provide, authorize access, or input individuals' information, including personal or other regulated data, for processing using the Services (iii) if any content could be subject to governmental regulation or may require security measures beyond those specified by Converge using the Services, you will not provide, allow access to, or input the content for processing using the Services unless Converge has first agreed in writing to implement additional security and other measures (iv) monitoring and controlling the activity of each of your users ("User"), (v) ensuring that there is no unauthorized access to the Services and notifying Converge promptly of any such access of which you become aware, (vi) the reliability, accuracy, quality, integrity and legality of all your data and the means by which you acquire the data, and (vii) ensuring that the use of the Services is in compliance with all applicable laws and regulations. Converge shall ensure that you will be solely responsible and liable for the acts and omissions of each User using the Services.

LIMITATIONS OF LIABILITY

Converge's entire liability for all claim related to the EULA will not exceed the amount of any actual direct damages incurred by you up to the amounts paid (if recurring charges, up to 12 months' charges apply) for the Service that is the subject of the claim, regardless of the basis of the claim.

Converge will not be liable to you (whether under the law of contact, the law of torts or otherwise) in relation to the contents of, or use of, or otherwise in connection with the Services:

- for any direct loss;
- for any indirect, special or consequential, exemplary, economic consequential damages loss; or
- for any business losses, goodwill, loss of revenue, income, profits or anticipated savings, loss of contracts or business relationships, loss of reputation or goodwill, or loss or corruption of information or data.
- These limitations apply collectively to Converge, affiliates, contractors, and suppliers.

These limitations of liability apply even if Converge has been expressly advised of the potential loss.

REASONABLENESS

By using the Services, you agree that the limitations of liability set out in this EULA disclaimer are reasonable. If you do not think they are reasonable, you must not use the Services.

HIGH RISK ACTIVITIES

THE SERVICES ARE NOT DESIGNED OR INTENDED FOR USE IN HAZARDOUS OR CRITICAL ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE OR IN ANY APPLICATION IN WHICH THE FAILURE OF THE SERVICES COULD LEAD TO DEATH, PERSONAL INJURY, OR PHYSICAL OR PROPERTY DAMAGE.

INFRINGEMENT CLAIMS

- If a third party asserts a claim against you that the Services infringes a patent or copyright, Converge will defend you against that claim and pay amounts finally awarded by a court against you or included in a settlement approved by you.
- To obtain Converge's defense against and payment of the infringement claims, you must promptly:
    (1) notify Converge in writing of the claim;
    (2) supply information requested by Converge; and
    (3) allow Converge to control, and reasonably cooperate in, the defense and settlement, including mitigation efforts.
- Converge has no responsibility for claims based on:
    (1) non-Converge products and services;
    (2) items not provided by Converge; or
    (3) any violation of law or third-party rights caused by your content, materials, designs, or specifications.

INDEMNITY

You hereby indemnify Converge and undertake to keep Converge indemnified against any losses, damages, costs, liabilities and expenses incurred or suffered by Converge arising out of any breach by you of any provision of these terms and conditions or arising out of any claim that you have breached any provision of these terms and conditions.

VARIATION

Converge may revise these terms and conditions from time-to-time. Revised terms and conditions will apply to the use of the Services from the date of the publication of the revised terms and conditions of this EULA. Please check this page regularly to ensure you are familiar with the current version.

ASSIGNMENT

Converge may not transfer, sub-contract or otherwise deal with Converge's rights and/or obligations under these terms and conditions without notifying you or obtaining your consent excepting that Converge may freely engage its whole-owned subsidiaries as listed below:

- Information Insights, LLC
- ExactlyIT, Inc.

You may not transfer, sub-contract or otherwise deal with your rights and/or obligations under these terms and conditions.

COMPLIANCE WITH LAWS

Each party is responsible for complying with:

(1) laws and regulations applicable to the business and content; and
(2) import, export and economic sanction laws and regulations, including defense trade control regime of any jurisdiction, including the International Traffic of Arms Regulations and those of the United States that prohibit or restrict the export, re-export, or transfer of products, technology, services or data, directly or indirectly, to or for certain countries, end uses or end users.

LAW AND JURISDICTION

- Both parties agree to the application of the law of the State of New York, United States, without regard to conflict of law principles.

- The rights and obligations of each party are valid only in the country of your business address.
- If you or any user exports or imports content or uses any portion of the Services outside the country of your business address, Converge will not serve as the exporter or importer, except as required by data protection laws.
- If any provision of the EULA are invalid or unenforceable, the remaining provisions remain in full force and effect.
- Nothing in this EULA affects statutory rights of consumers that cannot be waived or limited by contract.
- The United Nations Convention on Contracts for the International Sale of Goods does not apply to transactions under this EULA.

CAUSE OF ACTION

- No right or cause of action for any third party is created by this EULA or any transaction under it.
- Neither party may bring a legal action arising out of or related to the EULA more than two years after the cause of action arose.
- Neither party is responsible for failure to fulfill its non-monetary obligations due to causes beyond its control.
- Each party will allow the other reasonable opportunity to comply before it claims the other has not met its obligations.

GENERAL

- Converge does not undertake to perform any of your regulatory obligations or assume any responsibility for your business operation and you are responsible for your use of the Services.
- Converge is acting as an information technology provider only.
- Converge's direction, suggested usage, or guidance or use of the Services do not constitute medical, clinical, legal, accounting, or other licensed professional advice. You and your authorized users are responsible for the use of the Services within any professional practice and should obtain your own expert advice.
- Each party is responsible for determining the assignment of its and its affiliates' personnel and their respective contractors, and for their direction, control, and compensation.

ENTIRE AGREEMENT

These terms and conditions constitute the entire agreement between you and Converge in relation to your use of the Services and supersede all previous agreements in respect of your use of the Services.

EXHIBIT A

ACCEPTABLE USE POLICY

Coverage of this Policy
The following terms apply to your use of and access to any Converge services or products ("Services") made available by the Services. You agree to comply with this Acceptable Use Policy by using Services, which may be amended, modified or updated from time to time.

Your Internal Use. You will ensure your end users will use the Services solely for its internal business purposes; and neither you nor your end users will: (i) commercially exploit the Services by licensing, sub-licensing, selling, re-selling, renting, leasing, transferring, distributing, time sharing or making the Services available in the manner of a service bureau; (ii) create derivative works based on the Services; (iii) disassemble, reverse engineer or decompile the Services or any part thereof or permit others to do so; or (iv) access all or any part of the Services in order to build a product or service that competes with the Services.

Illegal or Harmful Use. You will only use Services for lawful purposes. You bear all responsibility for ensuring your own users comply with all applicable laws and regulations and appropriate conduct, without limitation, outlined in this AUP.

> **Offensive, Harmful or Illegal Content.** You may not publish or transmit via the Services any content or links to any content that Converge reasonably believes (i) is offensive and may be defamatory, obscene, abusive, excessively violent, threatening or harassing, invasive of privacy, objectionable or constitutes, fosters or promotes pornography; (ii) is harmful and is considered unfair or deceptive under consumer protection laws, such as pyramid schemes and chain letters, creates risks for a person or the public's safety or health, compromises national or local security, interferes with law enforcement investigations or improperly exposes trade secrets or other confidential or proprietary information of another person, or improperly exposes; or (iii) is illegal and may infringe upon another person's copyright, trade or service mark, patent, or other property right where permission was not first obtained by the owner of such rights, promotes illegal drugs, violates export control laws, relates to illegal gambling, or illegal arms trafficking, or is otherwise illegal or solicits conduct under laws applicable to you or Converge. Content "published or transmitted" via the Services includes Web content, e-mail, bulletin board postings, chat, and any other type of posting or transmission that relies on the Internet.
>
> **Network Abuse.** You may not use the Services to engage in, foster, or promote illegal, abusive, or irresponsible behavior, including, (i) unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network; (ii) monitoring data or traffic on

any network or system without the express authorization of the owner of the system or network; (iii) user of an Internet account or computer without the owner's authorization, interfering with the service to any user of the Services, including, without limitation, denial of service, mailing bombing or other flooding techniques to overload a system and broadcast attacks; (iii) collecting or using information without the consent of the owner of the information; (iv) use of any false, misleading, or deceptive TCP-IP packet header information to conceal the source or routing information of the network traffic or messages; (v) distributing software that covertly gathers information about or transmits information about a system or user; (vi) avoiding any limitations established by Converge using manual or electronic means to attempt to gain unauthorized access too, alter, or destroy information related to Converge or its customers; (vii) any conduct that is likely to interfere with, disrupt the integrity of or result in retaliation against the Services, or Converge's employees, officers or other agents.

Bulk or Commercial E-Mail. You must comply with the CAN-SPAM Act of 2003 and other laws and regulations applicable to bulk or commercial e-mail. You must not distribute, publish, or send through the Services: (i) any spam, including any unsolicited advertisements, solicitations, commercial e-mail messages, informational announcements, or promotional messages of any kind; (ii) chain mail; (iii) numerous copies of the same or substantially similar messages; (iv) empty messages; (v) messages that contain no substantive content; (vi) very large messages or files that disrupt a server, account, newsgroup, or chat service; or (vii) any message that is categorized as "phishing."

Likewise, you may not: (i) participate in spidering, harvesting, or any other unauthorized collection of e-mail addresses, screen names, or other identifiers of others or participate in using software (including "spyware") designed to facilitate such activity; (ii) collect responses from unsolicited messages; or (iii) use any of the Converge mail servers or another site's mail server to relay mail, such as, bulk e-mail, without the express permission of Converge, the account holder or the site. Converge may test and otherwise monitor your compliance with its requirements, and may block the transmission of e-mail that violates these provisions.

Security. Converge is responsible for maintaining the security of the infrastructure used to provision Services to you. It is the responsibility of you to understand and evaluate the security responsibilities of each party for Services against its security requirements including compliance regulations. You must take reasonable security precautions during its use of Services to configure and protect its operating systems, applications and data. Converge does not assume responsibility or accountability for such protections unless additional Services are mutually defined between Converge and you. You are responsible for protecting the confidentiality of any accounts used in connection with the Services and are encouraged to change associated passwords on a regular basis. Failure by you to protect the assigned environment may result in a security compromise by an unauthorized source. A compromised server or network device is potentially

disruptive to the Services and other customers. Therefore, Converge may, after notifying you of the situation, take your server or other device off line if Converge determines that it is being accessed or manipulated by a third party without your consent. You are solely responsible for the cost and resolution for any network or data breach introduced by you that affects systems, applications or data under your possession or control, or the Services and/or other Converge customers.

Vulnerability Testing. With Converge's express written consent, you may perform external vulnerability assessments and penetration tests on your designated IP addresses. You may not attempt to probe, scan, penetrate or test the vulnerability of a Converge system or network or to breach Converge's security or authentication measures, whether by passive or intrusive techniques that has not been specifically designated to you by Converge for its use. Converge maintains the right to block or shut down any vulnerability testing technique regardless of consent that interferes with Converge networks and its Services.

Copyrighted Material. Copyright infringement is a serious matter. You may not use the Services to download, publish, distribute, or otherwise copy in any manner any text, music, software, art, image, or other work protected by copyright law unless, (i) You have been expressly authorized by the owner of the copyright to copy/use the work in that manner; (ii) you are otherwise permitted by established United States copyright law to copy/use the work in that manner. Converge may terminate your service immediately if it is found to be infringing copyrights.

Copyright Infringement Notice (Digital Millennium Copyright Act). If you believe your copyright is being infringed by a person using the Services, please send your written notice of copyright infringement to:

Contracts & Compliance Department
Converge Technology Solutions Corp.
165 Barr Street
Lexington, KY 40507

Your notice must include the following:

- A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed;
- Identification of the copyrighted work claimed to have been infringed, or if multiple copyrighted works at a single site are covered by a single notification, a representative list of such works at that site;
- Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit Converge to locate the material;
- Information reasonably sufficient to permit Converge to contact you, such as an address, telephone number, and, if available, an e-mail address;

- A statement that you have a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, the copyright owner's agent, or the law;
- A statement that the information in the notification is accurate, and under penalty of perjury that you are authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Cooperation with Investigations and Legal Proceedings. Converge may, without notice to you, report to the appropriate authorities any conduct by you that you believe violates applicable criminal law. Converge will attempt to notify you if Converge is requested to; provide any information it has about you in response to a formal or informal request from a law enforcement or government agency, or in response to a formal request in a civil action that on its face meets the requirements for such a request. You must understand that there may situations that will prevent Converge from making notification or preventing such data from being released without your consent.

Other

- You must have valid and current information on file with its domain name registrar for any domain hosted on the Converge network.
- You may only use IP addresses assigned to it by Converge staff in connection with the Services.
- You agree that if the Converge IP numbers assigned to its account become listed on Spamhaus, Spews, NJABL or other abuse databases, you will be in violation of this AUP, and Converge may take reasonable action to protect its IP numbers, including suspension and/or termination of your Service, regardless of whether the IP numbers were listed as a result of your actions. Before taking any action to suspend or terminate your Service, Converge will investigate the matter and communicate with you regarding the possible causes of the problem and any reasonable actions that may be taken to absolve the IP numbers in question.

Consequences of Violation of AUP. Converge may without notice to you suspend its service or remove any content transmitted via the Service if it discovers facts that lead it to reasonably believe your Service is being used in violation of this AUP. You must cooperate with Converge's reasonable investigation of any suspected violation of the AUP. Converge will attempt to contact you prior to suspension of network access to your server(s), however, prior notification is not assured. In the event Converge takes corrective action due to a violation of the AUP, Converge shall have no liability to you or to any of your end users due to any corrective action that Converge may take (including, without limitation, suspension, termination or disconnection of Services).

You are strictly responsible for the violation of this AUP, including violation by its customers, users, and including violations that occur due to unauthorized use of your Services (but not including unauthorized use that results from Converge's failure to perform its obligations as

defined in the Services. Converge may charge you its hourly rate for AUP breach recovery (currently $350.00 USD) plus the cost of equipment and material needed to (i) investigate or otherwise respond to any suspected violation of this AUP, (ii) remedy any harm caused to Converge or any of its customers by the violation of this AUP, (iii) respond to complaints, including complaints 4 under the Digital Millennium Copyright Act, (iv) respond to subpoenas and other third party requests for information as described in the Agreement, and (v) have Converge's Internet Protocol numbers removed from any abuse database. No credit will be available under the SLA in Exhibit A, for interruptions of service resulting from AUP violations.

Amendments to AUP. The Internet is still evolving, and the ways in which the Internet may be abused are also still evolving. Therefore, Converge may from time to time amend this AUP in accordance with its Agreement to further detail or describe reasonable restrictions on your use of the Services. Inquiries regarding this policy should be directed to ATTN: Sr. Director of Risk and Compliance of Compliance Department.

Disclaimer. Converge is under no duty, and does not by this AUP undertake a duty, to monitor or police our customers' activities and disclaims any responsibility for any misuse of the Converge network. Converge disclaims any obligation to any person who has not entered into an agreement with Converge for services.