cellulant

Cellulant Data Processing Agreement

This **Data Processing Agreement** (the "DPA") between **Customer** (PII Controller) and Cellulant Kenya Limited (**Cellulant**) shall govern the relationship between the parties and applies to all Processing of Customer Data by Cellulant in order to provide the Contracted Services under all Agreements and any future Agreement(s). All capitalized terms used in this DPA and not defined shall have the meaning prescribed in the Agreement(s). The effective date of this DPA will be the date of the last party's signature.

This DPA sets out general specifications regarding the Customer Data processed by Cellulant in Exhibits 1-3, which shall apply to all Agreement(s). However, certain Contracted Services might require further specification or additional regulations which shall be agreed upon between the parties in the respective Service Agreement or Work Authorization (WA) and which shall prevail for the respective Service.

1. Definitions

1.1 **Act** means the Data Protection Act 2019, Laws of Kenya.

1.2 ***Adequate Country*** means a country providing an adequate level of protection pursuant to the Data Protection Laws, for example under GDPR - to a country in the European Economic Area or to one having an adequacy decision of the European Commission as set out in Art. 45 GDPR.

1.3 ***Agreement*** means the base terms or other Agreement(s) executed between Customer and Cellulant, such as the Cellulant Relationship Agreement including applicable Attachments, Statements of Work or other transaction documents.

1.4 ***Contracted Service(s)*** means all Deliverables, all testing, maintenance and support, all hosting and operation of any Cloud Service, and any other Services identified in an Agreement. or WA.

1.5 ***Controller*** means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Customer Data.

1.6 ***Data Breach*** means a suspected or actual breach of security or failure to establish safeguards leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data transmitted, stored, or otherwise processed.

1.7 ***Data Importer*** means a Sub processor not established in an Adequate Country.

1.8 ***Data Subject*** is the identified or identifiable natural person the Personal Data or Personally Identifiable Information (PII) is relating to.

1.9 ***Data Protection Law(s)*** means all data protection laws and regulations, including but not limited to the Act and the GDPR.

1.10 ***GDPR*** means the General Data Protection Regulation 2016/679.

1.11 **Customer *Data*** means all information, data, assets, documents, and data, including any Customer Personal Data, that Customer, Customer Personnel, a client, client's personnel, or any other person or entity, in connection with the Agreement(s), provides to Cellulant or uploads to or stores in a Contracted Service or Cloud Service, or to which Cellulant otherwise has access. Except as otherwise specified in a or Attachment, Cellulant will use Customer Data only as necessary to satisfy its obligations under the Agreement(s).

1.12 **Customer *Personal Data*** means the Personal Data which Cellulant is processing as Processor on behalf of Customer in order to provide the Contracted Services. Customer Personal Data includes both, Personal Data controlled by Customer and Personal Data Customer is Processing on behalf of Other Controllers as Processor.

1.13 MNO means Mobile Network Operator

1.14 ***Other Controller*** means any entity other than Customer that is Controller of the Customer Personal Data, such as Customer's affiliated companies or Customer's client's, their customers, or affiliated companies.

1.15 ***Personal Data*** means any information relating to an identified or identifiable natural person ('Data Subject or PII Principal'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Also, may be referred to as Personally Identifiable Information (PII).

1.16 ***Process or Processing*** means any operation or set of operations which is performed on Customer Data or on sets of Customer Data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.17 ***Processor*** means a natural or legal person, public authority, agency, or other body which processes Customer Data on behalf of the Controller.

1.18 ***Sub processor*** means any subcontractor engaged in delivering the Contracted Service and thereby Processing Customer Data.

1.19 ***Supervisory Authority*** means any regulatory authority, including but not limited to an independent public authority which is established pursuant to the Data Protection Laws.

1.20 ***Cellulant Affiliates*** means companies which are controlled by Cellulant, which control Cellulant, or which are under common control with Cellulant. "To control" or "to be controlled" means to hold, directly or indirectly, more than 50% of the respective shares with voting rights.

1.21 ***TOMs*** means the technical and organizational measures implemented by the Cellulant to ensure a level of security appropriate to the risk, compliance with Data Protection Laws and the protection of the rights of the Data Subjects.

2. Processing

2.1 Customer appoints Cellulant as Processor to process such Customer Data.

2.2 EXHIBIT 2 (Processing Details) generally sets out:

(a) the nature, purposes, and subject matter of the Processing;
(b) the duration of the Processing;
(c) categories of Data Subjects; and
(d) types of Customer Personal Data.

2.3 Cellulant shall not Process Customer Data for any purpose other than for the specific purpose of performing the Contracted Services, except as required by applicable law. Cellulant is prohibited from selling Customer Data (selling includes the definition(s) set forth in applicable Data Protection Laws (*i.e.,* Kenya Data Protection Act 2019)).

2.4 Cellulant will Process Customer Data for the sole purpose of providing the Contracted Services according to Customer's written instructions. The initial scope of Customer's instructions for the Processing of Customer Data is defined by the Agreements including, in particular, this DPA. Customer may provide further instructions that Cellulant has to comply with. In case Cellulant cannot accommodate an instruction, the parties shall work together in good faith to find an alternative solution. If Cellulant believes an instruction violates a Data Protection Law, Cellulant will inform Customer immediately.

2.5 Customer will serve as a single point of contact for Cellulant. Similarly, Cellulant will serve as a single point of contact for Customer and is solely responsible for the internal coordination, review and submission of instructions or requests from Customer to any Sub processors, except as specifically set out in the DPA.

2.6 Cellulant will comply with all Data Protection Laws related to the Contracted Services applicable to it.

3. Technical and Organizational Measures

3.1 Cellulant confirms that it has implemented and will maintain appropriate TOMs, specifically, the general TOMs set out in EXHIBIT 3.

3.2 The appropriateness of the TOMs is subject to technical progress and further development. If Customer requires changes to the TOMs or to the manner in which Cellulant implements these TOMs, such changes shall be implemented in accordance with the process set forth in Exhibit 3 (Technical and Organizational Measures).

3.3 Cellulant shall regularly monitor its compliance with the TOMs and will verify this monitoring and its compliance upon Customer's request.

4. Data Subject Rights and Requests

4.1 Cellulant will inform Customer without undue delay of requests from Data Subjects exercising their Data Subject rights (including but not limited to rectification, deletion and blocking of data) addressed directly to Cellulant regarding Customer Personal Data. Cellulant will not answer any requests from Data Subjects unless it is legally required or instructed by Customer in writing to do so.

4.2 If Customer is obliged to provide information regarding Customer Personal Data to Other Controllers or third parties (e.g. Data Subjects or the Supervisory Authority), Cellulant shall assist Customer in doing so immediately upon receiving notification from the Customer by providing all information and taking reasonable action as requested by Customer.

4.3 If a Data Subject brings a claim directly against Customer for damages suffered in relation to Cellulant's proven breach of this DPA or Data Protection Laws with regard to the processing of Customer Personal Data, Cellulant will indemnify and hold harmless Customer for any costs, charges, damages, expenses or losses arising from such a claim, limited to the direct loss incurred by the Data Subject provided that Customer has notified Cellulant about the claim and is giving the Cellulant the possibility to cooperate with Customer in the defense and settlement of the claim.

5. Third Party Requests and Confidentiality

5.1 Cellulant will not disclose Customer Data to any third party, unless authorized by Customer or required by law, in which case Cellulant shall provide prior notice to Customer of that legal requirement. If a government or Supervisory Authority demands access to Customer Data, Cellulant will notify Customer prior to disclosure unless such notification is prohibited by law.

5.2 Cellulant shall require all of its personnel authorized to process Customer Data to commit themselves to confidentiality and not Process such Customer Data for any other purposes, except on instructions from Customer and/or, if applicable, Other Controllers or unless required by applicable law. Such an obligation of confidentiality shall include annual security and privacy training and continue indefinitely. Upon request, Cellulant shall demonstrate proof of its compliance with this obligation without undue delay.

6. Information and Audit

6.1 Upon request, Cellulant is obliged to provide information in writing about the processing of Customer Data, including but not limited to the TOMs implemented and any Sub processors engaged.

6.2 If applicable, Cellulant shall maintain and annually renew the security certifications and Personal Data seals and marks set out in EXHIBIT 3. Upon request, Cellulant will provide Customer with the annual certifications and audit reports from accredited independent third-party auditors concerning the security measures used to provide the Contracted Services.

6.3 Cellulant shall allow for and contribute to audits, including inspections, conducted by Customer to demonstrate compliance with Cellulant's obligations set out in this DPA and the Data Protection Laws applicable to Cellulant in the performance of the Contracted Services. Cellulant can provide proof of the adherence to an approved code of conduct or an approved certification mechanism, or otherwise provide information to Customer which may be used as an element to demonstrate compliance with Cellulant's

obligations. Customer may reasonably assure itself of Cellulant's compliance at Cellulant's business premises involved in the Processing of Customer Data during Cellulant's normal business hours after prior notification. Cellulant will provide Customer access to Customer Data accordingly and/or access to its business premises involved in the Processing of Customer Data. To the extent Customer is mandating another auditor, such other auditor shall not be a direct competitor of Cellulant with regard to the respective Service and shall be bound to confidentiality.

7. Return or Deletion of Customer Data

Unless otherwise required by applicable law, Cellulant will, at Customer's choice, either delete (by rendering the Customer Data unreadable and unable to be reassembled or reconstructed) or return the Customer Data upon termination or expiration of the Agreement, or earlier upon request from Customer. Before termination or expiration of the Agreement, Cellulant shall contact Customer, requesting if the Customer Data shall be deleted or returned. If applicable, Cellulant will return the Customer Data within a reasonable period in a reasonable and common format upon receiving written instructions from Customer. At Customer's request, Cellulant shall certify to Customer in writing that the Customer Data has been deleted.

8. Sub processors

8.1 **Cellulant will notify the Customer on the engagement of Sub processors** (responsible for storage or transmission including MNOs)) Customer hereby explicitly approves the engagement of the Sub processors listed in EXHIBIT 1 Section 1(a). Cellulant will notify Customer in advance of any changes to Sub processors in accordance with EXHIBIT 1 Section 2.

8.2 Cellulant shall impose the same data protection obligations as set out in this DPA on any approved Sub processor prior to the Sub processor Processing any Customer Data. Cellulant remains responsible for its Sub processors and liable for their acts and omissions as for its own acts and omissions.

9. Transborder Data Processing

9.1 Cellulant will not transfer or disclose across borders (including by remote access) any Personal Data that is collected on behalf of Customer, received from Customer or its personnel or otherwise processed on behalf of Customer without obtaining prior written consent. In the event Cellulant requests written consent and Customer authorizes such transfer in writing, such transfer shall occur in accordance with applicable law. For clarity, by signing of this contract the Customer explicitly approves the Sub processors listed in Exhibit 1. Such approval shall constitute Customer's written authorization to transfer the Personal Data to the country in which the Sub processor is established in.

9.2 In the case of a transfer of Customer Personal Data across a country border, the parties shall cooperate to ensure compliance with the applicable Data Protection Laws. If the measures set out are not sufficient to comply with Data Protection Laws, the parties will work together in good faith to implement the additional legal requirements. To the extent there are legally required country specific privacy provisions (*e.g.,* country specific requirements) that must be inserted, the parties agree to promptly enter into an amendment to include such provisions.

10. Data Breach & Compliance

10.1 Cellulant will notify Customer without undue delay (and in no event later than 24 hours) after becoming aware of a Data Breach in respect of the Contracted Services. Cellulant will promptly investigate the Data Breach and will provide Customer with reasonable assistance to satisfy any legal obligations (including obligations to notify Supervisory Authorities or Data Subjects) of Customer in relation to the Data Breach.

10.2 Cellulant shall not inform or notify any third party about a Data Breach unless approved by Customer in writing or if required by law. Cellulant shall notify Customer in writing prior to distributing the legally required notification.

10.3 Cellulant will inform Customer without undue delay of any non-compliance with applicable Data Protection Laws or relevant contractual terms or in case of serious disruptions to operations or any other irregularities in the Processing of the Customer Data. Cellulant will promptly investigate and rectify any non-compliance as soon as possible and upon Customer's request, provide Customer with all information requested with regard to the non-compliance.

11. Assistance and Records

11.1 Considering the nature of Processing, Cellulant will assist Customer by having appropriate TOMs for the fulfillment of Customer's obligation to comply with the rights of Data Subjects. Cellulant shall assist Customer in ensuring compliance with obligations relating to the security of processing, the notification and communication of a Data Breach while taking into account the information available to Cellulant. Additionally, Cellulant will assist customers as further required by Data Protection Laws.

11.2 Cellulant will maintain an up-to-date record of the name and contact details of each Sub processor of Customer Data and, where applicable, the Sub processors' representative and data protection officer. Upon request, Cellulant will provide an up-to-date copy of this record to Customer.

12. General

12.1 Whenever this DPA is referring to written form, electronic form such as email shall be sufficient.

12.2 Customer and Cellulant agree that this DPA is part of the Agreement and is governed by its terms and conditions, unless otherwise required by applicable law. In case of conflict, the order of precedence in respect of the Processing of Customer Data shall be: this DPA and then the Agreement, unless otherwise set out in this DPA.

12.3 If an amendment to this DPA, including its Exhibits, is required in order to comply with applicable Data Protection Laws or comply with requirements set out by Customer's clients, Customer will provide an amendment to this DPA with the required changes to Cellulant. Both parties will work together in good faith to promptly execute a mutually agreeable amendment to this DPA reflecting the requirements.

12.4 This DPA shall not restrict any applicable Data Protection Laws. If any provision in this DPA is ineffective or void, this shall not affect the remaining provisions. The parties shall replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. In case a necessary provision is missing, the parties shall add an appropriate one in good faith.

12.5 The Parties agree that they shall each be responsible for all costs associated with their compliance of such obligations. Each Party is responsible and liable for its acts and omissions under this DPA.

12.6 This DPA is intended to constitute the data privacy and security terms for all Customers and/or Cellulant Affiliates which shall be fully incorporated, as necessary, in a separate agreement between such Affiliates. To the extent either Customer Affiliate or Cellulant Affiliate needs to execute an affiliate agreement or other document, Cellulant and the Customer will work together to promptly execute such documents or facilitate execution of such documents by its respective Affiliates. Cellulant agrees that its Cellulant Affiliates will reference this DPA in the affiliate Agreement, if necessary.

EXHIBIT 1
APPROVED SUBPROCESSORS

1. List of Sub processors

Cellulant uses the following Sub processors:

Name of Sub processor	Country
Africa Data Centre Nairobi	Kenya
Internet Solutions Data Centre	Kenya
Simbanet Data Centre	Tanzania
MIC Tanzania PLC	Tanzania
Amazon Web Services	Ireland Germany United Kingdom United States of America
Tutuka	South Africa
Smile Identity	Kenya
Cybersource	USA
Freshworks	USA
Seacom	Kenya
Liquid Telecom	Kenya

2. Means of notification of changes of Sub processors

Cellulant will notify Customer of any intended changes to Sub processors by Via emails to contact information provided in the contract or their successors in a substantially similar job role

EXHIBIT 2
PROCESSING DETAILS
Personal Data Only

As set out in Section 2.2 of the DPA, the categories of Data Subjects, types of Customer Personal Data, and Processing operations and nature of Processing are set out below. Cellulant agrees that, for specific Contracted Services the information set out in Exhibit 2 might require further specifications. Those specifications will be agreed in the Agreement, or transaction document and shall take precedence over the information set out below.

1. Data Subjects

The Customer Personal Data may concern the following categories of Data Subjects:

- Customer's employees (including temporary workers, volunteers, assignees, trainees, retirees, pre-hires/applicants)
- Other Controller's employees (including temporary workers, volunteers, assignees, trainees, retirees, pre-hires/applicants)
- Customer's (potential) clients
- Other Controller's (potential) clients
- Employees of Customer's (potential) clients
- Employees of Other Controller's (potential) clients
- Customer's business partners
- Other Controller's business partners
- Employees of Customer's business partners
- Employees of Other Controller's business partners
- Customer's visitors
- Other Controller's visitors
- Customer's subcontractors
- Other Controller's subcontractors
- Employees of Customer's subcontractors
- Employees of Other Controller's subcontractors
- Customer's agents, consultants, and other professional experts (contractors)
- Other Controller's agents, consultants, and other professional experts (contractors)

2. Types/Categories of Customer Personal Data

- general personal data (e.g. name; data and place of birth; age; (e-mail) address; phone number, photo, education; family status; nationality)
- online identification numbers (e.g. ID card number; passport number; personnel number, license number, IP addresses)
- banking data (e.g. account number, card information, account balance)
- physical characteristics (e.g. sex)
- factual circumstances/possession feature (e.g. license plate numbers)
- value judgements (e.g. employer references, recommendations)
- Location identifiers (*i.e.*, geo-location)
- Job category (*i.e.,* occupation, title)
- system access / usage / authorization data

3. Nature, purpose, and subject matter of the Processing / Processing Operations

The purpose and subject matter of the Processing is the provision of the Contracted Services.

The personal data transferred will be subject to the following basic processing activities:

- Data Storage (record, host, log, archive or otherwise store Customer Personal Data)
- Data Access (retrieve, copy, examine, modify, transport, scan, or otherwise access Customer Personal Data)
- Data Analysis (survey, test, study, interpret, organize, report, or otherwise analyze Customer Personal Data)

4. Duration of the Processing

The duration of the Processing corresponds to the duration of the respective Agreement and any applicable (s).

cellulant

EXHIBIT 3
TECHNICAL AND ORGANIZATIONAL MEASURES

This Exhibit 3 shall apply to Cellulant's processing of Customer Data.

Cellulant agrees that based on Customer requirements or the nature of the engagement, Customer may require Cellulant to agree to additional TOMs (Additional TOMs). The parties will mutually agree to the Additional TOMs in an Agreement or other transaction document. In the event of a conflict, the Additional TOMs shall take precedence over this Exhibit 3 for the specific Contracted Service.

Cellulant shall comply with the requirements of this Exhibit 3 in providing all Contracted Services, and by doing so protect Customer Data against loss, alteration, unauthorized disclosure, access, or other unlawful forms of processing. The requirements of this Exhibit 3 (Technical and Organizational Measures) extend to, but are not limited to, all Information Technology ("IT") applications, platforms, and infrastructure in and through which Cellulant creates and provides Contracted Services, including, but not limited, all development, testing, hosting, operations, and data center environments.

1. Data Protection

a. Cellulant will treat all Customer Data as confidential in accordance with Section 5 (Third Party Requests & Confidentiality) of the DPA.

b. Cellulant shall design security and privacy measures to protect and maintain the availability of Customer Data pursuant to the Agreement, including through its implementation, maintenance, and compliance with policies and procedures which require security and privacy by design, and secure operations, for all Contracted Services.

2. Security Policies

a. Cellulant will maintain and follow IT security policies and procedures that are integral to Cellulant's business and mandatory for all Cellulant Personnel. Cellulant will maintain responsibility and executive oversight for such policies and procedures, including formal governance and revision management of the policies and procedures, employee education on the policies and procedures, and compliance enforcement of the policies and procedures.

b. Cellulant will review its IT security policies and procedures at least annually and amend them as necessary to protect the Contracted Services and Customer Data.

c. Cellulant will maintain and follow standard, mandatory employment verification requirements for all new employee hires, and extend such requirements to all Personnel and Personnel of Cellulant Affiliates and wholly owned Cellulant subsidiaries. Those requirements will include criminal background checks, proof of identity validation, and any additional checks that Cellulant deems necessary, as permitted by law. Cellulant will periodically repeat and revalidate these requirements, as it deems necessary.

d. Cellulant will provide security and privacy education to its Personnel annually, and require all Personnel to certify each year that they will comply with Cellulant's ethical business conduct, confidentiality, and security policies, as set out in Cellulant's code of conduct or similar document. Cellulant will provide additional policy and process training to Personnel with administrative access to any components of the Contracted Services, with such training specific to their role and support of the Contracted Services, and as necessary to maintain required compliance and certifications.

3. Security Incidents

a. Cellulant will maintain and follow documented incident response policies consistent with NIST guidelines for computer security incident handling.

b. Cellulant will investigate any Data Breach and will define and execute an appropriate response plan.

c. Cellulant will provide notice of any Data Breach in accordance with Section 10.2 above and provide the Customer with reasonably requested information about such security incidents and the status of any Cellulant remediation and restoration activities.

4. Physical Security and Entry Control

a. Cellulant will maintain appropriate physical entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, to protect against unauthorized entry into Cellulant facilities. Cellulant will also control auxiliary entry points into such facilities, such as delivery areas and loading docks, and isolate those entry points from computing resources.

b. Cellulant will require authorized approval for access to controlled areas within its facilities and will limit access by job role. Cellulant will implement physical access controls that are consistent with industry best practices, to appropriately restrict entrance to controlled areas, will log all entry attempts, and retain such logs for at least one year (and will provide those logs to Customer upon request).

c. Cellulant will revoke access to facilities and controlled areas upon 1) separation of an authorized Personnel or 2) the authorized Personnel no longer having a valid business need for access. Cellulant will follow formal documented separation procedures that include, but are not limited to, prompt removal from access control lists and surrender of physical access badges.

d. Cellulant will ensure that any temporary access to a facility or controlled area within a facility, including for deliveries, is scheduled in advance, with upfront review and clearance by an authorized Cellulant employee. Cellulant will require that any person granted temporary access registers, providing proof of identity, before entering the facility. If Cellulant grants temporary access, its authorized employee will escort any such person while in the facility and any controlled areas.

e. Cellulant will take precautions to protect all physical infrastructure used to support the Contracted Services against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

5. Access, Intervention, Transfer, and Separation Control

a. Cellulant will maintain documented security architecture of networks that it manages in its operation of the Contracted Services. Cellulant will employ measures to prevent unauthorized network connections to systems, applications, and network devices, ensuring compliance with secure segmentation, isolation, and defense in-depth standards. Cellulant may use wireless networking technology in its delivery of the Contracted Services, but Cellulant must encrypt and require secure authentication for any such wireless networks.

b. Cellulant will maintain measures that are designed to logically separate and prevent any Customer Data from being exposed to or accessed by unauthorized persons. Further, Cellulant will maintain appropriate isolation of its production, non-production, and any other environments, and, if any Customer Data are transferred to a non-production environment (for example to reproduce an error), then Cellulant will ensure that all security and privacy protections in the non-production environment are equal to those in the production environment.

c. Cellulant will encrypt all Customer Data in transit and at rest (unless Cellulant demonstrates to Customer's reasonable satisfaction that encryption for Customer Data at rest is technically infeasible). Cellulant will also encrypt all physical media, if any, such as media containing backup files. Cellulant will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use associated with data encryption.

d. If Cellulant requires access to any Customer Data, Cellulant will restrict and limit such access to the least level required to provide and support the Contracted Services. Cellulant shall require that such access, including administrative access to any underlying components (i.e., privileged access), will be individual, role based, and subject to approval and regular validation by authorized Cellulant employees following segregation of duty principles. Cellulant will maintain measures to identify and remove redundant and dormant accounts with privileged access and will promptly revoke such access upon the account owner's separation or at the request of authorized Cellulant employees, such as the account owner's manager.

e. Consistent with industry standard practices, Cellulant will maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and measures requiring secure transfer and storage of such passwords and passphrases. Additionally, Cellulant will utilize multi-factor authentication for all non-console based privileged access to any Customer Data.

f. Cellulant will monitor use of privileged access and maintain security information and event management measures designed to 1) identify unauthorized access and activity, 2) facilitate a timely and

appropriate response to such access and activity, and 3) enable audits by Cellulant Customer (pursuant to its audit rights in this Agreement) and others of compliance with documented Cellulant policy.

g. Cellulant will retain logs in which it records, in compliance with its records retention policy, all administrative, user, or other access or activity to or with respect to Customer Data (and will provide those logs to Customer upon request). Cellulant will maintain measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of such logs.

h. Cellulant will maintain computing protections for systems, including end-user systems, containing any Customer Data, with such protections including, but not limited to: endpoint firewalls, full disk encryption, signature and non-signature based endpoint detection and response technologies to address malware and advanced persistent threats, time based screen locks, and endpoint management solutions that enforce security configuration and patching requirements.

i. Consistent with industry standard practices, Cellulant will maintain protections for data center environments where Customer Data are present or processed, with such protections including, but not limited to intrusion detection and prevention and denial of service attack countermeasures and mitigation.

6. Service and Systems Integrity and Availability Control

a. Cellulant will 1) perform security and privacy risk assessments at least annually; 2) perform penetration testing and assess vulnerabilities, including automated system and application security scanning and manual ethical hacking, before production release and annually thereafter, 3) enlist a qualified independent third-party to perform penetration testing at least annually, 4) perform automated management and routine verification of compliance with security configuration requirements for each component of the Contracted Services, and 5) remediate identified vulnerabilities or noncompliance with its security configuration requirements based on associated risk, exploitability, and impact. Cellulant will take reasonable steps to avoid disruption of Contracted Services when performing its tests, assessments, scans, and execution of remediation activities. Upon Customer's request, Cellulant will provide Customer with a written summary of Cellulant's then-most recent penetration testing activities, which report must at a minimum include the name of the offerings covered by the testing, the number of systems or applications in-scope for the testing, the dates of the testing, the methodology used in the testing, and a high-level summary of findings.

b. Cellulant will maintain policies and procedures designed to manage risks associated with the application of any changes to Contracted Services. Prior to implementing any change to a Contracted Service, including affected systems, networks, and underlying components, Cellulant shall document in a registered change request a description of and reason for the change, implementation details and schedule, a risk statement addressing impact to the Contracted Service and clients of the Contracted Service, expected outcome, rollback plan, and approval by authorized Cellulant employees.

c. Cellulant will maintain an inventory of all IT assets it uses in operating the Contracted Services. Cellulant will continuously monitor and manage the health (including capacity) and availability of such IT assets, the Contracted Services, and their underlying components.

d. Cellulant will build all systems that it uses in the development or operation of Contracted Services from predefined system security images or security baselines, which satisfy industry accepted best practices.

e. Without limiting Cellulant's obligations or Customer's rights under the Agreement with respect to business continuity, Cellulant will separately assess each Contracted Service for business and IT continuity and disaster recovery requirements pursuant to documented risk management guidelines. Cellulant shall ensure that each Contracted Service has, to the extent warranted by such risk assessment, separately defined, documented, maintained, and annually validated business and IT continuity and disaster recovery plans consistent with industry standard practices. Cellulant shall ensure that such plans are designed to deliver the specific Recovery Point and Time Objectives (RTO/RPO).

f. Cellulant will maintain measures designed to assess, test, and apply security advisory patches to the Contracted Services and associated systems, networks, applications, and underlying components within the scope of those Contracted Services. Upon determining that a security advisory patch is applicable and appropriate, Cellulant will implement the patch pursuant to documented severity and risk assessment guidelines. Cellulant's implementation of security advisory patches will be subject to its change management policy.

7. Amendment and Specific Performance

a. If a Customer notifies Cellulant that a modification to this Exhibit 3 (Technical and Organizational Measures) is necessary to address any requirement under applicable law or client obligation, then the parties will work together in good faith to promptly amend this Exhibit to include such modification.