cellulant

Supplier Data Processing Agreement

This **Data Processing Agreement** (the "DPA") between **Cellulant** (PII Controller) and [Insert name of Supplier] (**Supplier**) shall govern the relationship between the parties and applies to all Processing of Cellulant Data by Supplier 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 Cellulant Data processed by Supplier 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 Cellulant and Supplier, such as the Supplier 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 Cellulant 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, Cellulant 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 **Cellulant** ***Data*** means all information, data, assets, documents, and data, including any Cellulant Personal Data, that Cellulant, Cellulant Personnel, a client, client's personnel, or any other person or entity, in connection with the Agreement(s), provides to Supplier or uploads to or stores in a Contracted Service or Cloud Service, or to which Supplier otherwise has access. Except as otherwise specified in a or Attachment, Supplier will use Cellulant Data only as necessary to satisfy its obligations under the Agreement(s).

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

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

1.14 ***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).

1.15 ***Process or Processing*** means any operation or set of operations which is performed on Cellulant Data or on sets of Cellulant 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.

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

1.17 ***Sub processor*** means any subcontractor, including Supplier Affiliates, engaged in delivering the Contracted Service and thereby Processing Cellulant Data.

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

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

1.20 ***TOMs*** means the technical and organizational measures implemented by the Supplier 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 Cellulant appoints Supplier as Processor to process such Cellulant 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 Cellulant Personal Data.

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

2.4 Supplier will Process Cellulant Data for the sole purpose of providing the Contracted Services according to Cellulant's written instructions. The initial scope of Cellulant's instructions for the Processing of Cellulant Data is defined by the Agreements including, in particular, this DPA. Cellulant may provide further instructions that the Supplier has to comply with. In case Supplier cannot accommodate an instruction, the parties shall work together in good faith to find an alternative solution. If there is no alternative solution or Cellulant cannot accept an alternative solution, Cellulant may terminate the affected part of the Service by providing Supplier with a written notice. If Supplier believes an instruction violates a Data Protection Law, Supplier will inform Cellulant immediately.

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

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

3. Technical and Organizational Measures

3.1 Supplier 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 Cellulant requires changes to the TOMs or to the manner in which Supplier implements these TOMs, such changes shall be implemented in accordance with the process set forth in Exhibit 3 (Technical and Organizational Measures).

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

4. Data Subject Rights and Requests

4.1 Supplier will inform Cellulant 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 Supplier regarding Cellulant Personal Data. Supplier will not answer any requests from Data Subjects unless it is legally required or instructed by Cellulant in writing to do so.

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

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

5. Third Party Requests and Confidentiality

5.1 Supplier will not disclose Cellulant Data to any third party, unless authorized by Cellulant or required by law, in which case Supplier shall provide prior notice to Cellulant of that legal requirement. If a government or Supervisory Authority demands access to Cellulant Data, Supplier will notify Cellulant prior to disclosure unless such notification is prohibited by law. If Supplier is prohibited from notifying Cellulant, Supplier will take appropriate steps to challenge the prohibition through judicial action or other means where possible.

5.2 Supplier shall require all of its personnel authorized to process Cellulant Data to commit themselves to confidentiality and not Process such Cellulant Data for any other purposes, except on instructions from Cellulant 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, Supplier shall demonstrate proof of its compliance with this obligation without undue delay.

6. Information and Audit

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

6.2 If applicable, Supplier shall maintain and annually renew the security certifications and Personal Data seals and marks set out in EXHIBIT 3. Upon request, Supplier will provide Cellulant 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 Supplier shall allow for and contribute to audits, including inspections, conducted by Cellulant and, if applicable, Other Controller(s) and the respective Supervisory Authorities, or any other auditor mandated by Cellulant and/or Other Controllers to demonstrate compliance with Supplier's obligations set out in this DPA and the Data Protection Laws applicable to Supplier in the performance of the Contracted Services. Supplier can provide proof of the adherence to an approved code of conduct or an approved certification mechanism, or otherwise provide information to Cellulant which may be used as an element to demonstrate compliance with Supplier's obligations. Cellulant or Other Controllers may reasonably assure itself of Supplier's compliance at Supplier's business premises involved in the Processing of Cellulant Data during Supplier's normal business hours after prior notification. Supplier will provide Cellulant and, if applicable, Other Controllers access to Cellulant Data accordingly and/or access to its business premises involved in the Processing of Cellulant Data. To the extent Cellulant is mandating another auditor, such other auditor shall not be a direct competitor of Supplier with regard to the respective Service and shall be bound to confidentiality.

7. Return or Deletion of Cellulant Data

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

8. Sub processors

8.1 The engagement of Sub processors (including Supplier Affiliates) by Supplier requires Cellulant's explicit prior written approval. Cellulant hereby explicitly approves the engagement of the Sub processors listed in EXHIBIT 1 Section 1(a). Supplier will notify Cellulant in advance of any changes to Sub processors in accordance with EXHIBIT 1 Section 2.

8.2 Supplier 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 Cellulant Data Supplier 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 Supplier will not transfer or disclose across borders (including by remote access) any Personal Data that is collected on behalf of Cellulant, received from Cellulant or its personnel or otherwise processed on behalf of Cellulant without obtaining prior written consent. In the event Supplier requests written consent and Cellulant authorizes such transfer in writing, such transfer shall occur in accordance with applicable law. For clarity, if Cellulant approves a Sub processor in accordance with Section 8 (Sub processors) above, such approval shall constitute Cellulant'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 Cellulant 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 Supplier will notify Cellulant without undue delay (and in no event later than 24 hours) after becoming aware of a Data Breach in respect of the Contracted Services. Supplier will promptly investigate the Data Breach and will provide Cellulant with reasonable assistance to satisfy any legal obligations (including obligations to notify Supervisory Authorities or Data Subjects) of Cellulant and/or Other Controllers in relation to the Data Breach.

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

10.3 In case of a Data Breach within Supplier's area of responsibility or control,

a. Supplier shall be responsible for any costs incurred by Cellulant in providing notification of the Data Breach to applicable Supervisory Authorities or other government and relevant industry self-regulatory agencies, to the media (if required by applicable law) and to individuals whose Personal Data may have been accessed or acquired. Cellulant shall determine, in its sole discretion, whether notification of the Data Breach is to be sent to applicable government and relevant industry self-regulatory agencies, to the media (if required by applicable law) and to affected individuals.

b. if requested by Cellulant, Supplier shall establish and maintain at its own expense a call center to respond to questions from individuals whose Personal Data was involved in the Data Breach for a period of two year(s) after the date on which such individuals were notified of the Data Breach. Cellulant and Supplier shall work together to create the scripts and other Data to be used by call center staff when responding to inquiries by affected individuals. Alternatively, on written notice to Supplier, Cellulant may establish and maintain its own call center, in lieu of having Supplier establish a call center. Supplier shall reimburse Cellulant the actual costs incurred by Cellulant in connection with establishing and maintaining such call center.

c. Supplier shall reimburse to Cellulant the actual costs of providing credit monitoring and/or credit restoration services for two (2) years following the date of notice of the Data Breach to all individuals affected by the Data Breach who choose to register for such credit monitoring services.

10.4 Supplier will inform Cellulant without undue delay of any suspected 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 Cellulant Data. Supplier will promptly investigate and rectify any non-compliance as soon as possible and upon Cellulant's request, provide Cellulant with all information requested with regard to the suspected non-compliance.

11. Assistance and Records

11.1 Considering the nature of Processing, Supplier will assist Cellulant and other Controller(s) by having appropriate TOMs for the fulfillment of Cellulant's and/or Other Controllers' obligation to comply with the rights of Data Subjects. Supplier shall assist Cellulant and/or Other Controllers' in ensuring compliance with obligations relating to the security of processing, the notification and communication of a Data Breach and as applicable, the data protection impact assessment, including prior consultation with the responsible Supervisory Authority, if required, taking into account the information available to Supplier. Additionally, Supplier will assist Cellulant as further required by Data Protection Laws.

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

12. General

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

12.2 Cellulant and Supplier 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 Cellulant Data shall be: Exhibits to this DPA, 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 Cellulant's clients, Cellulant will provide an amendment to this DPA with the required changes to Supplier. Both parties will work together in good faith to promptly execute a mutually agreeable amendment to this DPA reflecting the requirements. In case Supplier is not able to accommodate the requested changes, Cellulant may terminate all or part of the Agreements and this DPA with thirty (30) days' written notice.

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 Supplier agrees that it shall be responsible for all costs associated with its compliance of such obligations. Supplier is responsible and liable for its acts and omissions under this DPA.

12.6 All damages arising under this DPA shall be deemed direct damages. Supplier's obligation to reimburse Cellulant or pay for remediation as provided herein is not conditioned on Supplier's insurance

covering such costs. Notwithstanding anything to the contrary in the Agreement, the limitation of liability set forth in the liability section of the base agreement shall not apply to losses or claims arising out of or relating to this DPA.

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

12.8 Supplier certifies and understands the restrictions in this DPA and shall comply with them.

EXHIBIT 1
APPROVED SUBPROCESSORS

1. Means of notification of changes of Sub processors

Supplier will notify Cellulant of any intended changes to Sub processors by via emails to following individual specified in contract or their successors in a substantially similar job role

PROCESSING DETAILS
Personal Data Only

As set out in Section 2.2 of the DPA, the categories of Data Subjects, types of Cellulant Personal Data, and Processing operations and nature of Processing are set out below. Supplier 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 Cellulant Personal Data may concern the following categories of Data Subjects:

- Cellulant'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)
- Cellulant's (potential) clients
- Other Controller's (potential) clients
- Employees of Cellulant's (potential) clients
- Employees of Other Controller's (potential) clients
- Cellulant's business partners
- Other Controller's business partners
- Employees of Cellulant's business partners
- Employees of Other Controller's business partners
- Cellulant's visitors
- Other Controller's visitors
- Cellulant's suppliers and subcontractors
- Other Controller's suppliers and subcontractors
- Employees of Cellulant's suppliers and subcontractors
- Employees of Other Controller's suppliers and subcontractors
- Cellulant's agents, consultants, and other professional experts (contractors)
- Other Controller's agents, consultants, and other professional experts (contractors)

2. Types/Categories of Cellulant 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. social security number; tax identification number; health insurance number; ID card number; passport number; personnel number, license number; matriculation number, IP addresses)
- banking data (e.g. account number, credit (card) information, account balance)
- physical characteristics (e.g. sex; hair-, eye colour; stature; size)
- factual circumstances/possession feature (e.g. license plate numbers)
- 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 Cellulant Personal Data)
- Data Access (retrieve, copy, examine, modify, transport, scan, or otherwise access Cellulant Personal Data)
- Data Analysis (survey, test, study, interpret, organize, report, or otherwise analyze Cellulant Personal Data)

4. Duration of the Processing

☒ The duration of the Processing corresponds to the duration of the respective Agreement and any applicable (s) unless otherwise stated in the contract.

cellulant

EXHIBIT 3
TECHNICAL AND ORGANIZATIONAL MEASURES

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

Supplier agrees that based on Cellulant or Other Controllers' requirements or the nature of the engagement, Cellulant may require Supplier 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.

Supplier shall comply with the requirements of this Exhibit 3 in providing all Contracted Services, and by doing so protect Cellulant 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 Supplier creates and provides Contracted Services, including, but not limited, all development, testing, hosting, operations, and data center environments.

1. Data Protection

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

b. Supplier shall design security and privacy measures to protect and maintain the availability of Cellulant 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.

c. Supplier will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with National Institute of Standards and Technology("NIST"), guidelines for media sanitization.

2. Security Policies

a. Supplier will maintain and follow IT security policies and procedures that are integral to Supplier's business and mandatory for all Supplier Personnel. Supplier 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. Supplier will review its IT security policies and procedures at least annually and amend them as necessary to protect the Contracted Services and Cellulant Data.

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

d. Supplier will provide security and privacy education to its Personnel annually, and require all Personnel to certify each year that they will comply with Supplier's ethical business conduct, confidentiality, and security policies, as set out in Supplier's code of conduct or similar document. Supplier 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. Supplier will maintain and follow documented incident response policies consistent with NIST guidelines for computer security incident handling.

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

c. Supplier will provide notice of any Data Breach in accordance with Section 10.2 above and provide Cellulant with reasonably requested information about such security incident and the status of any Supplier

remediation and restoration activities.

4. Physical Security and Entry Control

a. Supplier 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 Supplier facilities. Supplier 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. Supplier will require authorized approval for access to controlled areas within its facilities and will limit access by job role. Supplier 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 Cellulant upon request).

c. Supplier 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. Supplier 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. Supplier 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 Supplier employee. Supplier will require that any person granted temporary access registers, providing proof of identity, before entering the facility. If Supplier grants temporary access, its authorized employee will escort any such person while in the facility and any controlled areas.

e. Supplier 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. Supplier will maintain documented security architecture of networks that it manages in its operation of the Contracted Services. Supplier 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. Supplier may use wireless networking technology in its delivery of the Contracted Services, but Supplier must encrypt and require secure authentication for any such wireless networks.

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

c. Supplier will encrypt all Cellulant Data in transit and at rest (unless Supplier demonstrates to Cellulant's reasonable satisfaction that encryption for Cellulant Data at rest is technically infeasible). Supplier will also encrypt all physical media, if any, such as media containing backup files. Supplier 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 Supplier requires access to any Cellulant Data, Supplier will restrict and limit such access to the least level required to provide and support the Contracted Services. Supplier 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 Supplier employees following segregation of duty principles. Supplier 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 Supplier employees, such as the account owner's manager.

e. Consistent with industry standard practices, Supplier 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, Supplier will utilize multi-factor authentication for all non-console based privileged access to any Cellulant Data.

f. Supplier 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 Supplier, Cellulant (pursuant to its audit rights in this Agreement) and others of compliance with documented Supplier policy.

g. Supplier 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 Cellulant Data (and will provide those logs to Cellulant upon request). Supplier will maintain measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of such logs.

h. Supplier will maintain computing protections for systems, including end-user systems, containing any Cellulant 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, Supplier will maintain protections for data center environments where Cellulant 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. Supplier 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. Supplier will take reasonable steps to avoid disruption of Contracted Services when performing its tests, assessments, scans, and execution of remediation activities. Upon Cellulant's request, Supplier will provide Cellulant with a written summary of Supplier'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. Supplier 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, Supplier 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 Supplier employees.

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

d. Supplier 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 Supplier's obligations or Cellulant's rights under the Agreement with respect to business continuity, Supplier will separately assess each Contracted Service for business and IT continuity and disaster recovery requirements pursuant to documented risk management guidelines. Supplier 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. Supplier shall ensure that such plans are designed to deliver the specific Recovery Point and Time Objectives (RTO/RPO).

f. Supplier 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, Supplier will implement the patch pursuant to documented severity and risk assessment guidelines. Supplier's implementation of security advisory patches will be subject to its change management policy.

7. Service Provisioning

a. Supplier will support industry common methods of federated authentication for Cellulant user accounts, with Supplier authenticating such Cellulant user accounts by Cellulant centrally managed multi-factor Single

Sign-On (SSO), using OpenID Connect (OIDC) or Security Assertion Markup Language (SAML).

8. Product Certifications

a. Supplier will secure the certifications required by any agreement, within the time frames set forth in that agreement which are incorporated by reference in this Exhibit 3.

9. Amendment and Specific Performance

a. If Cellulant notifies Supplier 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.

b. If Supplier breaches any of its obligations under this Exhibit, then Cellulant is entitled to require Supplier's specific performance of its obligations, to fully remediate the harmful impact of any such breach, with such performance at Cellulant's reasonable direction and schedule. Supplier shall not refuse to provide such specific performance nor claim that the costs necessary to do so are subject to any damages disclaimer, exclusion, or cap in the Agreement.

10. Liability

a. Notwithstanding anything to the contrary in this Agreement, no provision of this Agreement shall be deemed or construed to disclaim, exclude, or limit any damages, costs, penalties, or other amounts arising from or in any way related to Supplier's breach of any obligation in this Exhibit.