Security Measures

The technical and organizational measures provided herein apply to all services and/or deliverables provided by Vendor (collectively, "**Contracted Services**") to JDA under the existing written or electronic agreement between JDA and the Vendor (the "**Agreement**") with regard to the processing of personal data.

1. Data Protection

a. Security measures for Contracted Services are designed to protect JDA Personal Data and to maintain the availability of such JDA Personal Data pursuant to the Agreement, including applicable Attachments, Statements of Work or other transaction documents, (collectively "Agreement Documents"). JDA is the sole controller for any personal data, and appoints Vendor as a processor to process such personal data (as those terms are defined in EU General Data Protection Regulation). Vendor will treat all JDA Personal Data as confidential by not disclosing JDA Personal Data except to Vendor employees, contractors, and subprocessors, and only to the extent necessary to deliver the Contracted Services, unless otherwise specified in Agreement Documents.

b. Vendor will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse.

2. Security Policies

a. Vendor will maintain and follow IT security policies and practices that are integral to Vendor's business and mandatory for all Vendor employees, including supplemental personnel.

b. Vendor will review its IT security policies at least annually and amend such policies as Vendor deems reasonable to maintain protection of Contracted Services and JDA Personal Data processed therein.

c. Vendor will maintain and follow its standard mandatory employment verification requirements for all new hires, including supplemental employees, and extend such requirements to wholly owned Vendor subsidiaries. In accordance with Vendor internal process and procedures, these requirements will be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by Vendor. Each Vendor company is responsible for implementing these requirements in its hiring process as applicable and permitted under local law.

d. Vendor employees will complete security and privacy education annually and certify each year that they will comply with Vendor's ethical business conduct, confidentiality, and security policies, as set out in Vendor's employee code of conduct. Additional policy and process training will be provided to persons granted administrative access to Contracted Services components that is specific to their role within Vendor's operation and support of the Contracted Services, and as required to maintain compliance and certifications stated in the relevant Agreement Documents.

3. Security Incidents

a. Vendor will maintain and follow documented incident response policies and will comply with data breach notification terms of the Agreement.

b. Vendor will investigate unauthorized access and unauthorized use of JDA Personal Data of which Vendor becomes aware (security incident), and, within the Contracted Services scope, Vendor will define and execute an appropriate response plan.

c. Vendor will promptly (and in no event later than 24 hours) notify JDA of a security incident or Personal Data Breach that is known or reasonably suspected by Vendor to affect JDA. Vendor will provide JDA with reasonably requested information about such security incident and status of any Vendor remediation and restoration activities.

4. Physical Security and Entry Control

a. Vendor 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 Vendor

facilities used to host the Contracted Services (data centers). Auxiliary entry points into data centers, such as delivery areas and loading docks, will be controlled and isolated from computing resources.

b. Access to data centers and controlled areas within data centers will be limited by job role and subject to authorized approval. Use of an access badge to enter a data center and controlled areas will be logged, and such logs will be retained for not less than one year. Vendor will revoke access to controlled data center areas upon a) separation of an authorized employee or b) the authorized employee no longer has a valid business need for access. Vendor 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.

c. Any person duly granted temporary permission to enter a data center facility or a controlled area within a data center will be registered upon entering the premises, must provide proof of identity upon registration, and will be escorted by authorized personnel. Any temporary authorization to enter, including deliveries, will be scheduled in advance and require approval by authorized personnel.

Vendor will take precautions to protect the Contracted Services physical infrastructure 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. Vendor will maintain documented security architecture of networks managed by Vendor in its operation of the Service. Vendor will separately review such network architecture, including measures designed to prevent unauthorized network connections to systems, applications and network devices, for compliance with its secure segmentation, isolation, and defense in depth standards prior to implementation. Vendor may use wireless networking technology in its maintenance and support of the Contracted Services and associated components. Such wireless networks, if any, will be encrypted and require secure authentication and will not provide direct access to Contracted Services networks. Contracted Services networks do not use wireless networking technology.

b. Vendor will maintain measures for Contracted Services that are designed to logically separate and prevent JDA Personal Data from being exposed to or accessed by unauthorized persons.

c. To the extent described in the relevant Agreement Documents, Vendor will encrypt JDA Personal Data not intended for public or unauthenticated viewing when transferring JDA Personal Data over public networks and enable use of a cryptographic protocol, such as HTTPS, SFTP, and FTPS, for secure transfer of JDA Personal Data to and from the Contracted Services over public networks.

d. Vendor will encrypt JDA Personal Data at rest when specified in Agreement Documents. If the Contracted Services includes management of cryptographic keys, Vendor will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

e. If Vendor requires access to JDA Personal Data, Vendor will restrict and limit such access to least level required to provide and support the Contracted Services. Such access, including administrative access to any underlying components (privileged access), will be individual, role based, and subject to approval and regular validation by authorized Vendor personnel following the principles of segregation of duties. Vendor 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 request of authorized Vendor personnel, such as the account owner's manager.

f. Consistent with industry standard practices, and to the extent natively supported by each component managed by Vendor within the Contracted Services, Vendor 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.

g. Vendor will monitor use of privileged access and maintain security information and event management measures designed to a) identify unauthorized access and activity, b) facilitate a timely and appropriate

response, and c) to enable internal and independent third party audits of compliance with documented Vendor policy.

h. Logs in which privileged access and activity are recorded will be retained in compliance with Vendor's records retention policy. Vendor will maintain measures designed to protect against unauthorized access, modification and accidental or deliberate destruction of such logs.

i. To the extent supported by native device or operating system functionality, Vendor will maintain computing protections for systems containing JDA Personal Data and all end-user systems that include, but may not be limited to, endpoint firewalls, full disk encryption, signature based antivirus and malware detection and removal that shall a) be regularly updated by central infrastructure and b) logged to a central location, time based screen locks, and endpoint management solutions that enforce security configuration and patching requirements.

6. Service Integrity and Availability Control

a. Vendor a) performs penetration testing and vulnerability assessments, including automated system and application security scanning and manual ethical hacking, before production release and annually thereafter, b) enlists a qualified independent third-party to perform penetration testing at least annually, c) performs automated management and routine verification of underlying components' compliance with security configuration requirements, and d) remediates identified vulnerabilities or noncompliance with its security configuration requirements based on associated risk, exploitability, and impact. Vendor will take reasonable steps to avoid Contracted Services disruption when performing its tests, assessments, scans, and execution of remediation activities.

b. Vendor will maintain policies and procedures designed to manage risks associated with the application of changes to its Contracted Services. Prior to implementation, changes to Contracted Services, including its systems, networks and underlying components, will be documented in a registered change request that includes a description and reason for the change, implementation details and schedule, a risk statement addressing impact to the Contracted Services and its clients, expected outcome, rollback plan, and documented approval by authorized personnel.

c. Vendor will maintain an inventory of all information technology assets used in its operation of the Contracted Services. Vendor will continuously monitor the health and availability of the Contracted Services and underlying components.

d. Each Contracted Services will be separately assessed for business continuity and disaster recovery requirements pursuant to documented risk management guidelines. Each Contracted Services will have, to the extent warranted by such risk assessment, separately defined, documented, maintained and annually validated business continuity and disaster recovery plans consistent with industry standard practices. Recovery point and time objectives for the Contracted Services, if provided, will be established with consideration given to the Contracted Services architecture and intended use, and will be described in the relevant Agreement Documents.

e. Vendor will a) backup systems containing JDA Personal Data daily, b) ensure at least one backup destination is at a remote location, separate from production systems, c) encrypt backup data stored on portable backup media and d) validate backup process integrity by regularly performing data restoration testing.

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