Security Measures

1 Asset Management

1.1 JDA maintains an inventory of IT assets supporting the Services including internal and external systems.

2 Governance

2.1 JDA maintains an Information Security Program (ISP) based on the ISO/IEC 27001 framework.

2.2 JDA's Security & Compliance Director is responsible for information security.

2.3 JDA requires that contractors meet the requirements of the Program, the same as JDA employees.

2.4 JDA requires contractors and employees to sign a Confidentiality Agreement and Acceptable Use Policy on hire.

3 Risk Management

3.1 JDA maintains risk management processes to identify, assess and manage risks to Customer Information and IT systems supporting the Services. JDA will promptly report material risks which may affect Customer Information or the Services to the Customer.

3.2 JDA conducts an information security risk assessment at least one time per year and manages risks to Customer Information and IT systems supporting the Services in accordance with documented risk management procedures.

3.3 JDA conducts vulnerability scans against infrastructure and applications in accordance with their risk to Customer, to help identify vulnerabilities and promptly remediates any security vulnerabilities and misconfiguration.

3.4 JDA conducts penetration testing of its external network at least one time per year using independent testing professionals and promptly remediates identified vulnerabilities.

3.5 JDA conducts penetration testing of its applications at least annually and promptly remediates identified vulnerabilities.

4 Awareness and Training

4.1 JDA ensures that Personnel complete information security awareness training and are made aware of their responsibilities with regards to information security and the handling of Customer Information at least one time per year.

4.2 JDA provides Personnel with clear instructions and awareness for using Customer Information and IT systems, including but not limited to, the following requirements:

a) Keep Confidential Information and IT equipment secure at all times, including when travelling or working out of the office or from home;

b) Keep Userids, passwords and PINs for IT systems and devices, confidential and protect them from unauthorized access;

c) Do not connect untrusted removable media devices to IT systems or laptops;

d) Keep devices used to access Customer Information and IT systems up-to-date with security updates;

e) Handle Customer Information in accordance with JDA's classification and documented handling procedures;

f) Only share Customer Information with authorized individuals on a need-to-know basis;

g) Encrypt Customer Personal Data when emailing or sharing externally;

h) Check before sending emails containing Customer Information that all the recipients are authorized to receive the Customer Information;

i) Be aware of phishing and do not click on links in emails or documents or provide any Customer Information over the phone without verifying the caller;

j) Do not use personal instant messaging services or personal email accounts to conduct Customer business or to share or receive Customer Information;

k) Be discreet when discussing Customer Information so you cannot be overheard and do not share Customer Information online, including using the social media, external social networks, instant messaging or blogging sites;

l) Maintain a clear desk and a clear screen so that Customer Information cannot be viewed or accessed by unauthorised individuals;

m) Do not leave Customer Personal Data unattended or on voicemails;

n) Securely dispose of paper and other media using correct procedures; and

o) Report security events and non-compliance to security policies promptly and without delay.

5 Access Control

5.1 JDA restricts physical and logical access to IT systems supporting the Services to only the minimum levels of access and privileges required to perform a function or role.

5.2 New access to network, systems, and data are approved and documented.

5.3 JDA assigns Users a unique ID; shared accounts are prohibited.

5.4 JDA implements identity and access management processes to control access and authenticate Users prior to granting access.

5.5 JDA uses Multi-Factor Authentication for remote User virtual private network access to systems containing Customer Personal Data.

5.6 JDA revokes access immediately for Users no longer working on the Services or those that no longer require access.

5.7 JDA reviews User accounts and their privileges on a regular basis, to verify that access to IT systems supporting the Services is correct.

5.8 JDA enforces the use of password complexity, minimum length of eight (8) characters, password changes every 60 days, and lockout after five (5) unsuccessful login attempts.

5.9 JDA ensures that remote access to IT systems and networks supporting the Services is restricted to only authorized individuals using secure entry-points and approved devices.

6 Data Center Security

6.1 JDA controls access to its data centers using a card-key access control system. Only appropriate Personnel are issued card-keys.

6.2 JDA requires visitors to its data centers to sign a visitor's log and visitors are escorted by JDA Personnel.

6.3 JDA ensures that security surveillance cameras are installed to record activity at the data center.

6.4 JDA disables card-keys to data centers within five (5) business days of an employee's termination or contractors end of assignment.

6.5 JDA assesses data centers for security requirements at least annually.

7 Data Security

7.1 JDA maintains procedures and controls to protect the security of Customer Personal Data (to the extent such Customer Personal Data or the environment under which it is stored is under Supplier's direct control) at every stage of its lifecycle from creation through processing, storage and disposal.

7.2 JDA enforces full-disk encryption on portable devices accessing Customer Information.

7.3 JDA encrypts Customer Personal Data in transit.

7.4 JDA maintains the security of systems and User laptops using standardized builds that include a hardened operating system, malware protection, and host-based security software. Only JDA-owned and managed laptops are allowed to connect to JDA's network and systems.

7.5 Configuration changes are limited to authorised individuals, in accordance with documented change management procedures and using approved systems and tools.

7.6 JDA will not send Customer Personal Data via email, instant messaging, or unapproved corporate collaboration tools.

7.7 If Customer Personal Data is stored on removable media, it is hardware encrypted and protected by a password.

7.8 On request, JDA will securely delete Customer Information from IT systems in accordance with current industry standards such as NIST 800-88 or an equivalent.

8 Application Security

8.1 JDA will not use Customer information for testing without the prior consent of Customer.

9 Operational Security

9.1 JDA maintains IT systems in a timely manner, in accordance with change management procedures.

9.2 JDA restricts access for remote maintenance to authorized Users performing approved maintenance, using authorized devices and tools.

9.3 Management conducts and documents a monthly review of system availability to help ensure compliance with Service Level Agreements (SLAs).

9.4 A 24-hour on-call procedure is implemented to provide support for production systems.

9.5 Monitoring software on production servers and applications automatically alerts personnel of error conditions.

9.6 Commercial anti-virus software is loaded on production servers to mitigate the risk of virus threats.

9.7 Production Windows servers are set to automatically update virus definition files.

9.8 Production servers are constructed through the completion of a build process. The build process is documented via a completed "build checklist."

10 Security Monitoring & Detection

10.1 JDA's security department is responsible for security monitoring and detection activities.

10.2 JDA maintains content filtering technologies to monitor connections to the internet.

10.3 JDA monitors CERT notifications that may affect any element of its IT systems and patch systems in accordance with a documented procedure that prioritizes the remediation of vulnerabilities based on risk.

10.4 JDA's security detection processes materially comply with all applicable requirements and maintain the privacy and civil liberties of Customer Users.

11 Incident Response

11.1 JDA maintains security incident response plans to manage eesponse to security events, and these are tested on at least an annual basis.

11.2 JDA will report confirmed breaches of Customer Information or the environment under which it is stored (to the extent the same is under Supplier's direct control) to Customer within 48 hours from the time JDA confirmed the breach of Customer Information.

11.3 JDA assesses security events and suspected incidents against defined criteria and responds to incidents in such a way that takes into consideration their potential impact to the Customer and the Customer's Affiliates.

11.4 JDA will consult with Customer prior to conducting forensic investigation following an incident affecting Customer Information or the environment under which it is stored (to the extent the same is under Supplier's direct control) and conduct investigations in accordance with legal requirements for preserving evidence. JDA will keep Customer apprised of the forensic investigations and remediation.

11.5 JDA will contain and mitigate incidents in accordance with documented incident management procedures and response plans.

11.6 JDA will mitigate newly identified vulnerabilities. Any vulnerabilities that cannot be fixed, that could have a material impact on the security of Customer Information will be reported to Customer.

11.7 JDA will conduct post incident reviews to identify root-causes and identify actions required to minimize the risk of similar incidents re-occurring. Response strategies and plans will be updated in response to any lessons learned.

12 Third Party Risk Management

12.1 JDA's security department maintains a third-party risk management program to ensure that third parties maintain security controls at least as stringent as JDA's security controls and continually assess the third party on a regular basis in accordance with its risk level as defined by JDA.

12.2 Third parties are obligated, by contractual agreement, to maintain security controls at least as stringent as JDA's security policies dictate.

12.3 Third parties are obligated, by contract, to securely delete data at the end of contract.

12.4 JDA will not use third-party cloud-hosted services to store or process Customer Personal Data without prior written consent of Customer.

13 Compliance

13.1 JDA conducts an annual compliance assessment of its ISP that is provided to the Customer on request. JDA may rely on existing independent third party audit reports or certifications (e.g. ISO27001 or SSAE 18) where the security requirements are equivalent in all material respects to those contained in the ISP.

13.2 JDA will support the Customer and/or the Customer's agent in assessing JDA's compliance with the ISP by completing a questionnaire one time per year.