virtusa

Vendor Information Security Addendum

1 Scope

Information security controls that Virtusa's Vendors must adopt when (a) on ongoing basis accessing Virtusa facilities, networks, and/or information systems (b) having custody of Virtusa/Virtusa's client hardware assets. Vendor is responsible for compliance to these terms by its personnel and subcontractors. Additional security compliance requirements may be specified in Vendor's agreement, appendices, or statements of work.

2 Acceptable use of Virtusa information assets and facility

2.1 Vendor must have a Non-Disclosure Agreement with Virtusa in place and comply with requirements of that agreement.

2.2 Vendor must establish and maintain Information security policies and program to ensure confidentiality of data and to ensure Virtusa/Virtusa's client data is secured, and adequate controls are implemented to prevent any data leakage or breaches

2.3 When a vendor employee works at Virtusa/Virtusa's client environment the vendor employee should adhere to the controls implemented and established by Virtusa.

2.4 Vendor employees should complete Virtusa Security First training within a day of getting access to Virtusa NT ID.

2.5 Vendor's access shall be restricted to those areas of Virtusa/Virtusa's client premises, and information which is specifically authorized by Virtusa.

2.6 Vendor's access to Virtusa/Virtusa's client premises and information shall be given only in relation to the mutually agreed services to be rendered.

2.7 Vendor shall not process or otherwise make use of Virtusa/Virtusa's client information, for any purpose other than that which is directly required to provide the agreed services.

2.8 Vendor shall ensure Virtusa/Virtusa's client assets are protected from misuse/mishandle at all times.

2.9 Vendor, its personnel or subcontractors shall not unless otherwise authorized by Virtusa store any confidential and proprietary information of Virtusa, its customers, its Vendors/vendors, its employees or its subcontractors and other agents.

2.10 Vendor shall Vendor shall update their Information security Policies and procedures at least annually or based on need/any new vulnerabilities or threats.

2.11 Vendor employee shall not access, upload, download, circulate, transmit, store or create any obscene, indecent, vulgar or inappropriate material on or through Virtusa/Virtusa's client systems or network or any resource provided by Virtusa/Virtusa's client.

2.12 Vendor shall provide appropriate awareness education and information security training and regular updates on organizational policies and procedures to its resources as relevant to their job functions.

3 Employee Background Check

3.1 Vendor shall conduct a background check (BGC) on its employees who are assigned to render services to Virtusa/Virtusa's client. The BGC shall be conducted at Vendor's cost and shall be completed before commencing the services to Virtusa. Unless otherwise agreed, the BGC components shall be as per Vendor's current standards and practices.

3.2 The Vendor shall provide a written statement to Virtusa/Virtusa's client confirming that the employee has successfully completed the background check in accordance with its screening requirements.

4 Security breaches involving Vendor personal

4.1 Upon any known potential or actual breach of the Virtusa Security Requirements or any obligations or duties owed by the vendor/vendor employees to Virtusa/Virtusa's client relating to the confidentiality, integrity or availability of Confidential Information or Personal Data (a "Data Security Breach"), in the most expedient time possible under the circumstances and at its expense the vendor shall

- Investigate the Data Security Breach to identify, prevent and mitigate the effects of the Data Security Breach and to carry out any recovery or other action necessary to remedy the Data Security Breach
- As soon as possible and in any event within twenty-four (24) hours notify Virtusa of the breach which includes (and follow-up with a detailed description in writing, including the cause of the breach, remedial action taken and the potential consequences of the breach). In case of privacy breach notification shall include (type of data that was the subject of the Data Security Breach and the identity of each affected person as soon as such information can be collected or otherwise becomes available)
- Conduct or support Virtusa in conducting investigations and analysis that Virtusa requires.
- Implement any additional actions or remedial measures which Virtusa considers necessary as a result of the breach
- Support Virtusa in any notification of the breach to Regulators and/or Data Subjects

4.2 Any critical security breaches/incidents involving Virtusa, or its client data should be reported within 4 hours of identification

5 Sub-Contractor engagement

5.1 The Vendor shall not sub-contract any of its services that it is obligated to perform under this agreement without prior written consent of Virtusa. Where the Vendor sub-contracts its obligations with the consent of Virtusa, it shall do so only by way of written agreement with the sub-contractor(s) which imposes the same obligations on the sub-contractor(s) as are imposed on the Vendor under this Agreement. Where the sub-contractor(s) fails to fulfil its obligations under such written agreement, the Vendor shall remain fully liable to Virtusa for the performance of the sub-contractor's obligations under such agreement.

6 Return of assets

6.1 At any time during the term of this Agreement at the Virtusa's request or upon the termination or expiration of this Agreement for any reason, it is the responsibility of the vendor to return all the assets given by Virtusa to the Vendor resources during the time of the contract.

6.2 It is the responsibility of the Vendor to return all the assets given by Virtusa when the vendor resource is separated/Terminated from the Vendor organization.

6.3 When the vendor resource offboarded from the project, it is the responsibility of the Vendor company to return all Virtusa assets used by the vendor employee during the time of the project.

7 Right to Audit

7.1 Virtusa reserves the right to perform an audit, if required and appropriate, yet not without prior written notification to the vendor, and without creating a business disturbance for the Vendor. Assessment may be performed by Virtusa and/or by Virtusa nominated third party and the information obtained during the assessment shall be treated with confidentiality within Virtusa.

8 Indemnity

8.1 Vendor shall defend, indemnify and hold harmless Virtusa, any subsidiary and affiliate thereof and their respective officers, directors, agents and employees harmless from and against all claims, damages, liabilities, costs, losses and expenses, including reasonable attorneys' fees and expenses arises out of or from any loss as a result of breach of this Vendor Information Security Addendum Appendix-B or any breach of confidentiality or intellectual property rights or breach of applicable law by the Vendor.

Company Name: _____

Name: _____

Signed By: _____

Date: _____