CURIA SECURITY ADDENDUM

CYBERSECURITY REQUIREMENTS

1. Cybersecurity Policy & Governance

1.1 Seller/Vendor shall create, implement, and maintain a cybersecurity program that meets or exceeds industry standards and that includes without limitation, appropriate policies, governance structures, staffing, monitoring and assessment procedures. Seller/Vendor's written program shall be approved by the Seller/Vendor's Chief Information Officer and at a minimum, updated annually.

2. Cybersecurity Assessments

2.1 CURIA reserves the right to perform, either itself or through an authorized representative, a questionnaire-based cybersecurity assessment not more than once per calendar year relating to the services provided by Seller/Vendor to CURIA and the requirements set forth in this Agreement.

2.2 CURIA shall provide Seller/Vendor with advance notice of a questionnaire-based cybersecurity assessment.

2.3 CURIA shall provide all assistance reasonably required to perform a questionnaire-based cybersecurity assessment based upon requirements set forth in this Agreement.

2.4 CURIA will be responsible for CURIA's costs associated with the questionnaire-based cybersecurity assessment. In no event will CURIA be responsible for any Seller/Vendor costs associated with the assessment.

2.5 Seller/Vendor shall remedy any identified and agreed-to cybersecurity deficiencies that are not in accordance with this Agreement in a timely manner at its own expense.

3. Incident Response

3.1 Seller/Vendor shall have a comprehensive incident response program that includes defined roles and responsibilities and covers the monitoring, detection and response to potential threats and incidents, as well as reporting of suspicious activity and weaknesses.

3.2 Seller/Vendor shall immediately report all Cybersecurity Incidents to CURIA's Cybersecurity Operations by email (itsecurity@curiaglobal.com) of a Cybersecurity Incident as defined below. To the extent available, Seller/Vendor shall include the

following in the email notification but not delay notification while the information is being gathered:

- Description of the nature and scope of the suspected Cybersecurity Incident
- Potential impact on the delivery of services to CURIA
- Potential impact on personal data, financial data, and other confidential information as defined in this Agreement or existing CDA between the parties including the number of subjects and records impacted
- Status on steps taken to mitigate the incident and minimize reoccurrence
- Name and contact details of the Cybersecurity leader and data protection officer

Definition: "Cybersecurity Incident" means any attempted or actual breach of security that results in the attempted, accidental or unlawful access, destruction, loss, alteration, or unauthorized disclosure of CURIA data, in the possession, custody or control of Seller/Vendor, its Affiliates and their respective directors, officers, employees, and contractors or the ability to deliver the contracted goods or services to CURIA. Examples of a Cybersecurity Incident include, but are not limited to, computer system breach; unauthorized access to, or use of, systems, software, or data; unauthorized changes to systems, software, or data; loss or theft of equipment storing institutional data; denial of service attack; interference with the intended use of information technology resources; and comprised user accounts.

3.3 Seller/Vendor shall promptly investigate all Cybersecurity Incidents and conduct internal forensic analysis and mitigation of all incidents, or shall as needed engage an external forensic incident response organization for such purpose.

4. Identity and Access Management

4.1 Seller/Vendor restricts system access only to authorized users with proper segregation of duties in accordance with the principle of least privilege.

4.2 Seller/Vendor performs user access reviews on a periodic basis to ensure user access is commensurate with the user roles and responsibilities.

4.3 Seller/Vendor shall have a formal approval mechanism to grant and revoke user access (privileged as well as non-privileged) to systems that store, transmit, access, or process CURIA data or have direct connectivity to the CURIA network.

4.4 Seller/Vendor restricts privileged and administrator access to appropriate users within the IT department who are responsible for the ongoing support and maintenance of the IT systems.

4.5 Seller/Vendor enforces strong password configuration requirements via a password management policy that is in alignment with industry best practices.

4.6 Seller/Vendor employs strong authentication protocols that effectively protect user accounts from being compromised through common exploits including, but not limited to, brute force attacks, password cracking tools, default passwords, dictionary attacks.

5. Network Security

5.1 Seller/Vendor configures firewalls and other network boundary devices to deny all access to the internal networks and only allow traffic based on defined rules.

5.2 Seller/Vendor deploys network intrusion detection/prevention technology to monitor and detect any abnormal network activity.

5.3 Seller/Vendor performs external network vulnerability assessments/penetration tests on the networks supporting services provided to CURIA and tracks through to completion all issues and findings identified during the external network vulnerability assessments/penetration tests.

5.4 Seller/Vendor implements and maintains VPN and multi-factor authentication for all users gaining remote access to CURIA data and systems.

6. Third Party Management

6.1 Seller/Vendor maintains a complete inventory of third parties who store, transmit, access or process CURIA data. This inventory tracks the inherent risk rating for each set of services being provided by the third party and the systems and data to which they have access.

6.2 Seller/Vendor monitors third party compliance with security requirements outlined in the agreement between the third party and Seller/Vendor.

6.3 Seller/Vendor has a formal third-party risk management policy or an equivalent policy/procedure that covers onboarding, monitoring and termination for third party providers.

7. Asset Management

7.1 Seller/Vendor maintains an accurate and up-to-date inventory of all software.

7.2 Seller/Vendor maintains a secure disposal procedure to provide sanitization of electronic media prior to reuse or disposal.

7.3 Seller/Vendor maintains a documented procedure for the build and maintenance of all servers, endpoints, etc.

8. Endpoint Security

8.1 Seller/Vendor ensures that CURIA data remains encrypted while in transit and at rest on Seller/Vendor-managed end point.

8.2 Seller/Vendor maintains a patch management policy and deploys patches based on their criticality levels and timelines established in the patch management policy.

8.3 Seller/Vendor deploys anti-malware/virus (AV) protection on all of its endpoints (i.e., servers, workstations, and mobile devices where possible). Seller/Vendor configures the AV policy so that malware and virus signatures are automatically updated, and real-time detection is enabled so that malicious software and files can be identified and quarantined as quickly as possible. Additionally, users do not have the ability to disable or adjust the policy setting of the AV software.

8.4 Seller/Vendor deploys an internet content filtering solution to restrict access to non-work related websites (i.e. social networking, personal email, data sharing).

8.5 Seller/Vendor implements and maintain an Email content filtering mechanism to remove or quarantine incoming emails with high risk file types (such as executables).

8.6 Seller/Vendor logs and monitors activities at the network and host level for all systems supporting services provided to CURIA.

9. Corporate Security Physical Security

9.1 Seller/Vendor has a physical security policy that governs the physical security of the organization and retention timelines for various facility related logs.

9.2 To the extent Seller/Vendor has deemed necessary for its operations, Seller/Vendor has CCTV cameras deployed at critical entry points and checkpoints throughout its applicable facilities.

9.3 To the extent Seller/Vendor has deemed necessary for its operations, Seller/Vendor issues physical IDs (badges or smart cards) for all staff who are permitted unescorted physical access to their applicable facilities. Seller/Vendor’s physical security team provisions access to designated areas of the organization's facilities based on the principle of least privilege in accordance with the staff's department and job function. The physical security team only issues badges and provisions physical access after

receiving authorization from Human Resources (HR) (or the Vendor Management office (VMO) for contractors). Additionally, the organization diligently revokes access when required.

10. Governance & Human Resources

10.1 Seller/Vendor maintains a formal Information Security Training and Awareness program that educates internal and external stakeholders on the organization's Information Security Policy, Procedures, and Standards. The Training and Awareness program comprises (a) general user training and (b) role-based security training for stakeholders in sensitive business and IT roles (e.g., executive leaders, IT system and database administrators, developers, etc.).

10.2 All employees, contractors, subcontractors, or agents of Seller/Vendor performing work under the Agreement shall have successfully completed state and federal security background screenings, as permitted by law.