Gates Foundation

INFORMATION SECURITY REQUIREMENTS ("*ISRs*")

1. APPLICATION

These ISRs are a part of the written or electronic agreement ("***Agreement***") for goods, deliverables, or services ("***Services***") between the Gates Foundation ("***Foundation***") and the individual or entity providing Services ("***You***"), when the Agreement references or incorporates these ISRs. Foundation and You are individually a "***Party***" and together the "***Parties.***" References to the Foundation and You will also include that Party's Affiliates as applicable to the Services. Except as provided below, these ISRs apply when in the course of the Services You access Foundation Information Systems, Process Personal Data, or host Sensitive Information, and will continue to apply as long as You do so. In the event of a conflict between these ISRs and the Agreement, the ISRs will control with respect to activities governed by the ISRs.

2. DEFINITIONS

In these ISRs, capitalized terms have the meanings set forth in the Agreement or, if not defined in an Agreement, as set forth below.

a. "***Affiliate***" means, with respect to a Party, any legal entity that controls, is controlled by, or is commonly controlled by or with a Party. "***Control***" means having more than 50% ownership or the right to direct the management of the entity.

b. "***Confidential Information***" whether written or oral means: (i) information relating to the Foundation's trustees, directors, strategies, finances, investments, grants, contracts, program-related investments, operations, facilities, events, guests, or security; (ii) Foundation employee and third-party information (including Personal Data); and (iii) any other information that the Foundation labels or indicates should be treated as confidential or which, under the circumstances of disclosure, ought to be treated as confidential.

c. "***Data Protection Laws***" means any laws, rules, regulations, and regulatory guidance, guidelines, and requirements relating to data privacy, data security, and the Processing of Personal Data applicable to a Party providing the Services, exercising its rights, or fulfilling its obligations under the Agreement.

d. "***Dispose***" means to return, securely destroy, delete, or permanently erase (on all forms of recordation or storage) any Sensitive Information in Your possession, custody, or control in a manner that complies with all applicable laws and makes the Sensitive Information unreadable or undecipherable through any means.

e. "***Foundation InfoSec***" means the Foundation's Information Security Department, which You will contact at infosec@gatesfoundation.org as required by the terms of these ISRs and as otherwise instructed by the Foundation.

f. "***Information Systems***" means equipment (including computers, servers, mobile devices, and cloud services), networks, and systems within the Party's possession, custody, or control (including through the Party's Personnel) (i) in which Sensitive Information is accessible, stored, or transmitted, or (ii) through which You or Your Personnel may have direct or indirect access to the Foundation's Information Systems.

g. "***Personal Data***" means any data or information that constitutes personal data or personal information under Data Protection Laws, including any information relating to an identified or identifiable natural person.

h. "***Personnel***" means the trustees, directors, officers, employees, contractors, subcontractors, consultants, contingent workers, representatives, agents, Affiliates, and any individuals managing or performing Services.

i. "***Process***" or "***Processing***" means any operation or set of operations performed on Personal Data, including access, collection, use, storage, disclosure, erasure, or destruction.

j. *"**Security Event**"* means an unauthorized occurrence that:

   i. actually or imminently jeopardizes the confidentiality, integrity, or availability of Foundation Sensitive Information or Foundation's Information Systems, or

   ii. is a violation or credible threat to violate (a) Foundation security policies, procedures, or acceptable use policies, or (b) laws or regulations related to information.

By way of example, the term Security Event includes any of the following: malware infection, ransomware attack, cyber and denial-of-service attack, and interference with information technology systems or process operation.

k. "***Sensitive Information***" means Confidential Information, Personal Data, other information that the Foundation labels or indicates should be treated as sensitive, and all backups or other copies.

3. YOUR INFORMATION SECURITY PROGRAM

You will implement and maintain appropriate technical and organizational measures included in a written information security program *(*Your "***Information Security Program***"), that includes legal, administrative, physical, policy, training, and state-of-the-art technical measures designed to:

a. ensure the security, confidentiality, privacy, availability, and integrity of Sensitive Information,

b. protect against any anticipated threats or hazards to the security, confidentiality, privacy, availability, or integrity of Sensitive Information,

c. protect against unauthorized access to, or use, disclosure, loss, alteration, or destruction of Sensitive Information both at rest and in-transit,

d. ensure the proper Disposal of Sensitive Information,

e. ensure compliance with applicable laws, standards, and policies, and

f. ensure that You and Your Personnel comply with Your Information Security Program and these ISRs.

You will designate an individual to be responsible and accountable for Your Information Security Program and for responding to the Foundation's inquiries regarding information security. Upon request, You will provide the Foundation with a written, detailed description of Your Information Security Program, including any written policies, procedures, and updates.

4. NETWORK AND COMMUNICATIONS SECURITY

You will ensure that:

a. Your actual and attempted connectivity to the Foundation's Information Systems will be only through the Foundation's security gateways and firewalls and only through the Foundation's authorized security procedures, which can be obtained from Foundation InfoSec,

b. You will not access, and will not permit unauthorized persons or entities to access, the Foundation's Information Systems without the Foundation's express written authorization, and any such actual or attempted access will be consistent with the Foundation's authorization,

c. You will take the utmost care to protect the security of any credentials and other means of access to the Foundation's Information Systems from unauthorized access or use, and treat the same as Sensitive Information, and

d. You will take appropriate measures to ensure that Your Information Systems that connect to the Foundation's Information Systems, and anything You provide to the Foundation, do not contain any computer code, programs, mechanisms, or programming devices designed to, or that would, enable the disruption, modification, deletion, damage, deactivation, disabling, harm or otherwise be an impediment, in any manner, to the operation of the Services or the Foundation's Information Systems, and You will immediately notify Foundation InfoSec of any vulnerabilities thereto.

5. LOGICAL ACCESS SECURITY

To safeguard Your and Your Personnel's access to Sensitive Information, You will implement authentication methods that incorporate multifactor authentication and are compliant with industry best practice and Data Protection Laws. Each of Your Personnel accessing Foundation Sensitive Information must have unique accounts and credentials and must not share accounts. Your Personnel will only be allowed access to the Sensitive Information to the extent required to perform the Services under the Agreement.

6. PHYSICAL SECURITY

All Sensitive Information must be contained in secure, environmentally controlled storage areas that You own, operate, or contract for.

7. ENCRYPTION

You will encrypt Sensitive Information, both at rest and in-transit, consistent with applicable industry best practice and guidance under Data Protection Laws relating to information security. You will not transmit any unencrypted Sensitive Information over the internet or a wireless network.

8. TRAINING

You will establish, maintain, and conduct formal security awareness training for Your Personnel who may access Foundation Information Systems or Process Sensitive Information. Your Personnel must receive such training prior to granting them permission to access, use, or otherwise Process Sensitive Information or the Foundation's Information Systems and annually thereafter. For the term of the Agreement, You will retain records documenting the completion of the trainings and make the documentation available for review by the Foundation on request.

9. DISPOSAL OF INFORMATION

You will Dispose of all Sensitive Information in Your possession, custody, or control upon the earlier of (a) termination or expiration of the Agreement, (b) the Foundation's request, or (c) or when You no longer need such Sensitive Information to fulfill the purpose for which You obtained it. If requested by the Foundation, You will provide a written acknowledgment that You have Disposed of all Sensitive Information (or specific Sensitive Information, if so requested).

Notwithstanding the foregoing, You may retain copies of Sensitive Information to the extent required to comply with applicable legal and regulatory requirements, provided, that (i) You shall restrict the access to and Processing of such Sensitive Information to the extent necessary to meet the requirements of such legally required obligations, and (ii) such Sensitive Information will remain subject to the terms and conditions of the Agreement and these ISRs. If the Sensitive Information includes Personal Data, the Agreement terms governing the disposal of Personal Data will control. A Party's rights and obligations under this provision will be continuous and survive the expiration or termination of the Agreement.

10. PENETRATION TESTING

You will engage, at Your own expense, a third-party vendor to perform penetration and vulnerability testing ("***Penetration Tests***") with respect to Your Information Systems (a) at least annually, and (b) following a Security Event upon the Foundation's request. Penetration Tests will probe for design, configuration, and functionality weaknesses and vulnerabilities in applications, network perimeters, or other infrastructure elements as well as weaknesses or vulnerabilities in process or technical countermeasures relating to Your Information Systems that could be exploited. Penetration Tests will identify, at a minimum, the following security vulnerabilities: invalidated or un-sanitized input; broken access control; broken authentication and session management; cross-site scripting flaws; buffer overflows; injection flaws; improper error handling; insecure storage; denial of service; insecure configuration management; proper use of SSL/TLS; proper use of encryption; and anti-virus reliability and testing.

If a Penetration Test reveals any high or very high security issues, You will do the following at your cost and expense:

a) prepare and deliver to the Foundation a detailed plan for remedying all the deficiencies leading to the security issues ("***Remedial Plan***"), which will include: (i) details of actions You will take to correct the deficiencies; and (ii) target dates for successful correction of the deficiencies. You will deliver the Remedial Plan to the Foundation within a reasonable period of time following identification of the deficiencies based on the nature and complexity of the deficiencies to be remedied, not to exceed thirty (30) calendar days.

b) engage the testing company to perform an additional Penetration Test within a reasonable period of time to ensure continued resolution of identified deficiencies and notify Foundation InfoSec with the results.

c) as requested by the Foundation, You will produce a report confirming the resolution of the deficiencies.

11. SECURITY AUDITS AND ASSESSMENTS

The Foundation may review Your Information Security Program prior to the commencement of Services and from time to time during the term of the Agreement. During the performance of the Services, from time to time

with prior written notice, the Foundation, at its own expense, may perform, or have performed, an on-site audit of Your Information Security Program, Your Information Systems, and Your facilities during normal business hours, provided that the Foundation will conduct no more than one such audit during any 12-month period or following a Security Event.

In lieu of an on-site audit, upon request by the Foundation, You will complete, within forty-five (45) calendar days of receipt, an information security assessment questionnaire provided by the Foundation or its designee regarding Your Information Security Program. You will, at Your own expense, cause a nationally recognized, independent certified public accounting or cybersecurity firm to conduct a SOC Type II audit or other independent controls assessment of Your Information Security Program ("***Security Audit***") at least annually, and provide a copy of the results of each Security Audit to Foundation InfoSec.

If a Security Audit reveals any deficiencies in Your Information Security Program, You will prepare and deliver to the Foundation a Remedial Plan which will include: (a) details of actions You will take to correct the deficiencies; and (b) target dates for successful correction of the actions to correct the deficiencies. You will deliver the Remedial Plan to Foundation InfoSec within a reasonable period of time following identification of the deficiencies based on the nature and complexity of the deficiencies to be remedied, not to exceed thirty (30) calendar days. As requested by the Foundation, You will produce a report confirming the resolution of the deficiencies. You will bear all costs and expenses associated with correcting all deficiencies.

12. NOTICE OF SECURITY EVENT

Upon discovery of a Security Event, You will (a) immediately commence all reasonable efforts to contain, investigate, correct the causes and remediate the results of the Security Event, (b) notify Foundation InfoSec and the Foundation's Legal Department (legal@gatesfoundation.org) as soon as practicable, but in no event more than three (3) calendar days following discovery of any Security Event, and (c) provide such further information and assistance as may be reasonably requested by the Foundation.

If a Security Event may require You, on behalf of the Foundation, to notify any third party, then (a) You will not provide such notices without the Foundation's prior written approval, unless otherwise required by law, and (b) You will provide the Foundation an opportunity to review, revise, and approve of the notifications You prepared prior to dissemination.

13. EXPENSES AND COSTS

You will reimburse the Foundation for all reasonable costs the Foundation incurs in responding to, and mitigating damages caused by a Security Event, including all costs of notice to individuals, regulatory authorities, and the media, as well as consumer remediation services.

14. INDEMNIFICATION

Without limitation to any other indemnification obligations set forth under the Agreement, You shall defend, indemnify, and hold harmless the Foundation and its successors, trustees, directors, officers, employees, and contractors from any and all losses, damages, liabilities, fines, penalties, costs, and expenses, including reasonable attorneys' fees and court costs, in any way arising from or caused by a Security Event or Your failure to comply with Your obligations set forth in these ISRs. In the event of a Security Event, the Foundation's damages shall not be subject to any limitation of damages and liability provision set forth in the Agreement.