Children of the Caribbean Foundation

INFORMATION SECURITY REQUIREMENTS ("ISRs")

1. DEFINITIONS

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

"*Agreement*" means the written or electronic agreement between Service Provider and the Foundation that references and incorporates these ISRs.

"*Confidential Information*" whether written, oral, or observed, means: (a) information relating to Foundation's directors, officers, strategies, finances, investments, grants, contracts, program-related investments, facilities, events, guests, or security; (b) employee and third-party information (including personal information) that the Foundation must treat as confidential or private; and (c) 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.

"Data Protection Laws" means all data protection and privacy laws applicable to a party in exercising its rights or fulfilling its obligations under the Agreement.

d. "Foundation" means the Children of the Caribbean Foundation and, if applicable, its affiliates.

e. "Foundation's Information Systems" means equipment (including computers, mobile devices, and cloud services), networks, and systems within the Foundation's possession, custody, or control (including through the Foundation's employees, contingent workers, vendors, contractors, consultants, service providers, representatives, or agents) where Sensitive Information is accessible, stored, or transmitted.

f.“Personal Data” or equivalent term has the meaning provided in the Agreement. If not defined in the Agreement, it shall mean any data that relates to an identified or identifiable natural person.

g.“Sensitive Information” means Confidential Information, Personal Data, and other information that the Foundation labels or indicates should be treated as sensitive.

h. “Service Provider’s Information Systems” means equipment (including computers, mobile devices, and cloud services), networks, and systems within Service Provider’s possession, custody, or control (including through Service Provider’s Personnel or other third parties) where Sensitive Information is accessible, stored, or transmitted or through which Service Provider’s Personnel may have access to the Foundation’s Information Systems.

i. “Service Provider” means the service provider, vendor, contractor, or consultant that is a party to, and providing services under, the Agreement and, if applicable, its affiliates.

j. “Service Provider’s Personnel” means Service Provider’s directors, officers, employees, vendors, service providers, subcontractors, consultants, sub-processors, contingent workers, representatives, agents, and affiliates.

2. SERVICE PROVIDER’S INFORMATION SECURITY PROGRAM

Service Provider will establish, maintain, and comply with a written information security program (“Service Provider’s Information Security Program”) that includes legal, administrative, physical, policy, training, and technical measures designed to: (a) ensure the security, confidentiality, and integrity of Sensitive Information; (b) protect against any anticipated threats or hazards to the security, confidentiality, 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 return or disposal of Sensitive Information in accordance with Section 9 (Disposal of Information) of these ISRs; (e) ensure compliance with applicable laws, standards, and policies in accordance with Section 14 (Compliance with Laws and Standards) of these ISRs; and (f) ensure that Service Provider’s Personnel comply with Service Provider’s Information Security Program and the requirements set forth in these ISRs. Service Provider will designate an individual to be responsible and accountable for Service Provider’s Information Security Program. Such individual will respond to the Foundation’s inquiries regarding information security. Upon request, Service Provider will provide the Foundation with a written, detailed description of Service Provider’s Information Security Program, including any written policies, procedures, and updates.

3. NETWORK AND COMMUNICATIONS SECURITY
Service Provider will ensure that: (a) Service Provider's connectivity to the Foundation's Information Systems and all attempts at the same will be only through the Foundation's security gateways/firewalls and only through the Foundation's authorized security procedures, which can be obtained from the Foundation's Information Security Department at adminisrator@caribbeanchild.com; (b) Service Provider 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; and (c) Service Provider will take appropriate measures to ensure that Service Provider's Information Systems which connect to the Foundation's Information Systems, and anything provided 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 Service Provider will immediately notify the Foundation at administrator@caribbeanchild.com of any vulnerabilities thereto.

4. LOGICAL ACCESS SECURITY
Service Provider will implement strong, industry standard authentication methods for accessing Sensitive Information, including multifactor authentication. All individuals accessing Foundation Sensitive Information must have unique accounts. Account sharing is not allowed under any circumstances. Individuals working for or on behalf of the Service Provider will only be allowed access to the Foundation data if their job function, as stipulated by the work order or agreement, requires it.

5. PHYSICAL SECURITY
All Sensitive Information, including data backups, must be contained in secure, environmentally controlled storage areas owned, operated, or contracted for by Service Provider.

6. ENCRYPTION
Service Provider will encrypt Sensitive Information both at rest and in-transit. Service Provider will not transmit any unencrypted Sensitive Information over the internet or a wireless network, and will not store any Sensitive Information on any mobile computing device, such as a laptop computer, USB drive or portable data device, except where there is a business necessity and then only if the mobile computing device is protected by industry standard encryption.

7. SUB-PROCESSORS
The Service Provider will ensure that any sub-processors engaged by Service Provider to process Sensitive Information are subject to the same data protection obligations as set out in these ISRs.

8. TRAINING

Service Provider must establish, maintain, and conduct formal security awareness training for Service Provider's Personnel who may access or use Sensitive Information or the Foundation's Information Systems. Service Provider's Personnel must receive such training prior to granting them permission to access or use Sensitive Information and/or the Foundation's Information Systems and annually thereafter. Documentation confirming that these trainings have been completed must be retained by Service Provider for the duration of the Agreement (or so long as Service Provider has access to, possession, custody, or control of Sensitive Information) and made available for review by the Foundation on request.

9. DISPOSAL OF INFORMATION

Upon termination or expiration of the Agreement or earlier upon the Foundation's request or when it is no longer needed to fulfill the purpose for which it was obtained, Service Provider will destroy or permanently erase (on all forms of recordation) any Sensitive Information in Service Provider's possession, custody, or control in a manner that complies with applicable laws and makes such Sensitive Information unreadable or undecipherable through any means. If requested by the Foundation, Service Provider will acknowledge in writing that all such Sensitive Information has been returned, destroyed, or permanently erased. Notwithstanding the foregoing, Service Provider may retain copies of Sensitive Information to the extent required to comply with applicable legal and regulatory requirements, provided, however, in which event the Service Provider 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 that such Sensitive Information will remain subject to the terms and conditions of the Agreement and this ISR.If the Sensitive Information includes Personal Data, the Agreement terms governing the disposal of Personal Data will control.

10.PENETRATION TESTING

Service Provider will engage, at Service Provider's own expense and at least one time per year, a third party vendor to perform penetration and vulnerability testing ("Penetration Tests") with respect to Service Provider's Information Systems Penetration Tests will probe for design and/or functionality weaknesses in applications, network perimeters, or other infrastructure elements as well as weaknesses in process or technical countermeasures relating to Service Provider's 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 (XSS) 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. Within a reasonable period after the annual Penetration Test has been performed, Service

Provider will notify the Foundation at administrator@caribbeanchild.com if such Penetration Testing reveals any high or very high deficiencies in Service Provider's information systems. Service Provider then will prepare and deliver to the Foundation a detailed plan for remedying all the deficiencies ("Remedial Plan"), which will include: (a) details of actions Service Provider will take to correct the deficiencies; and (b) target dates for successful correction of the actions to correct the deficiencies. Service Provider 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. Service Provider will bear all costs and expenses associated with correcting all deficiencies. To the extent that high level and/or medium level security issues were revealed during a particular Penetration Test, Service Provider will subsequently engage, at Service Provider's own expense, the Testing Company to perform an additional Penetration Test within a reasonable period thereafter to ensure continued resolution of identified security issues and will notify the Foundation with the results thereof.

11.SECURITY AUDITS AND ASSESSMENTS

The Foundation may review Service Provider's 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 Service Provider's Information Security Program, Service Provider's Information Systems, and Service Provider's facilities during normal business hours, provided that the Foundation will conduct no more than one such audit during any 12-month period or following an incident or breach. In lieu of an on-site audit, upon request by the Foundation, Service Provider will complete, within forty-five (45) days of receipt, an information security assessment questionnaire provided by the Foundation or its designee regarding Service Provider's Information Security Program. Service Provider will, at Service Provider's 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 Service Provider's Information Security Program ("Security Audit") at least annually, and provide a copy of the results of the Security Audit to the Foundation at administrator@caribbeanchild.com upon completion of each Security Audit. If such Security Audit reveals any deficiencies in Service Provider's Information Security Program, Service Provider will prepare and deliver to the Foundation a detailed plan for remedying all the deficiencies ("Remedial Plan"), which will include: (a) details of actions Service Provider will take to correct the deficiencies; and (b) target dates for successful correction of the actions to correct the deficiencies. Service Provider 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. Service Provider will bear all costs and expenses associated with correcting all deficiencies.

12.NOTICE OF BREACH

In the event of any actual or apparent theft, unauthorized use or disclosure of any Sensitive Information, Service Provider will immediately commence all reasonable efforts to investigate and correct the causes and remediate the results thereof and, as soon as practicable, but in no event more than three (3) days following discovery of any event described in this Section, provide the Foundation notice thereof via administrator@caribbeanchild.com and such further information and assistance as may be reasonably requested. If the Sensitive Information includes Personal Data, the Agreement terms governing the disposal of Personal Data will control.

13. INSURANCE

Without limiting in any way Service Provider's indemnification obligations under the Agreement, Service Provider will maintain at Service Provider's expense (and require and ensure that any of Service Provider's Personnel or other third party that Service Provider subcontract with or allow to access or use Sensitive Information or allow to access or use Service Provider's Information Systems in any manner that might allow access to or use of Sensitive Information, also maintains at its or Service Provider's expense): a minimum of $5,000,000 (per claim and in the aggregate) of privacy and security liability/cyber liability insurance that covers cyber, privacy, and security risks, including, but not limited to, damages arising from (a) a security event; (b) a breach of privacy no matter how it occurs; (c) a failure to protect Sensitive Information from misappropriation, release or disclosure; (d) a denial or loss of service; or (e) introduction, implantation, receipt, or spread of malicious software code. For claims-made coverage, the retroactive date will precede the first date Service Provider accesses or uses Sensitive Information, and Service Provider will maintain insurance for three (3) years following the term of the Agreement. Service Provider will submit to the Foundation, whenever requested, a certificate of insurance that evidences the required insurance coverages and names the Foundation as an additional insured on all policies. Service Provider will provide thirty (30) days' advance written notice to the Foundation at administrator@caribbeanchild.com in the event any adverse material change in its insurance coverage.

14.COMPLIANCE WITH LAWS AND STANDARDS

Service Provider will comply at all times with: (a) all Data Protection Laws relating to information security; and (b) all applicable industry standards and regulatory guidance relating to information security.

15.SURVIVAL

The provisions of these ISRs apply so long as Service Provider has access to Sensitive Information and/or the Foundation's Information Systems.