Smithsonian Institution
Privacy and Security Clause

1. Definitions: The definitions included in this Clause are applicable to performance of the statement of work. Other terms and conditions of this contract, purchase order, or agreement are not changed by this Clause. **(a) Breach:** A confirmed loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for an other than authorized purpose, have access or potential access to Smithsonian Data in a usable form whether physical or electronic. **(b) Cardholder Data Environment (CDE):** The people, processes and technologies that store, process, or transmit cardholder data or Payment Card Industry (PCI) sensitive authentication data by, or on behalf of, the Smithsonian. **(c) Cloud:** Computing services provided on-demand via a shared pool of configurable resources (e.g. networks, servers, storage, applications, and services) instead of via separate dedicated computing resources. **(d) Information Technology (IT) Security Incident:** Any action that threatens the confidentiality, integrity, or availability of Smithsonian IT resources, whether located inside or outside of the Smithsonian, or any activity that violates Smithsonian IT Security policies. IT resources include computer hardware and software, data, communication links, mobile devices, digitized assets, automated processes, physical computing environments, and associated personnel. **(e) Payment Application:** An application, system, software, or website used to electronically process, store, or transmit cardholder data or PCI sensitive authentication data as defined by the PCI Security Standards Council (SSC). See https://www.pcisecuritystandards.org/pci_security/glossary#Pm. **(f) Personally Identifiable Information (PII):** Information about individuals, which may or may not be publically available, that can be used to distinguish or indicate an individual's identity, and any other information that is linked or linkable to an individual, such as medical, educational, financial or employment information. It includes sensitive PII (sPII), a subset of PII defined as certain PII data elements that, if disclosed or used in combination with other data, could lead to harm to the individual (e.g., identity theft with the intention to do financial harm). **(g) Privacy Incident:** A suspected loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users are suspected of having access or potential access to PII or sPII in a usable form, whether physical or electronic, for an other than authorized purpose. **(h) Public-Facing Software:** An application, system, software, or website used by members of the public. **(i) Smithsonian Data:** Any physical or electronic information collected, processed, or stored by or on behalf of the Smithsonian. This includes, but is not limited to, PII.

2. If the Contractor is permitted access to Smithsonian Data in any form:[1/] **(a)** The Smithsonian retains sole ownership of, and unrestricted rights to, all Smithsonian Data. (**b**) Contractor shall maintain, transmit, and retain in strictest confidence, and prevent the unauthorized duplication, use and disclosure of Smithsonian Data. **(i)** The Contractor shall only access, maintain, use, and disclose Smithsonian Data to the extent necessary to carry out the requirements of this contract. **(ii)** The Contractor shall not use Smithsonian Data for testing or training purposes. **(iii)** The Contractor shall only provide Smithsonian Data to its authorized employees, contractors, and subcontractors and those Smithsonian employees, contractors, and subcontractors who have a valid business need to know such information in order to perform duties consistent with this contract. **(iv)** Contractor shall ensure that all Smithsonian Data is protected from unauthorized access, disclosure, modification, theft, loss, and destruction. **(v)** The Contractor shall not disclose Smithsonian Data without the Smithsonian's advance written authorization. If Contractor receives a legal request (such as a subpoena), or becomes subject to a legal requirement or order to disclose Smithsonian Data, the Contractor shall **(1)** immediately notify the Contracting Officer's Technical Representative (COTR) of it and afford the Smithsonian the opportunity to contest such disclosure, **(2)** assert the confidential nature of the Smithsonian Data and **(3)** cooperate with the Smithsonian's reasonable requirements to protect the confidential and proprietary nature of Smithsonian Data. **(c)** The Contractor and Contractor's employees who have access to Smithsonian network/systems shall, when requested by the COTR, complete SI-provided privacy and security training course(s), sign a nondisclosure agreement, sign a conflict of interest agreement, sign an acknowledgement of the requirements in this contract, provide fingerprints, pass a background check, and provide notice or the results of that background check to the COTR. The content and timing of the course(s), agreement, or background check shall be substantially similar to one that would be required of a Smithsonian employee with access to similar Smithsonian Data. **(d)** Contractor shall not transfer access to any Smithsonian Data in the event of a Contractor merger, acquisition, or other transaction, including sale in bankruptcy, without the prior written approval of the Contracting Officer. **(e)** Contractor shall provide the Smithsonian reasonable access to Contractor facilities, installations, technical capabilities, operations, documentation, records, databases, and personnel, and shall otherwise cooperate with the Smithsonian to the extent required to carry out an audit for compliance of the requirements in this contract.

3. If the Contractor uses, collects, maintains, stores, or shares Smithsonian Data in any form:[2/] **(a)** Contractor shall, as requested by the COTR, complete, or assist Smithsonian staff with the completion of, a privacy review which might include providing requested information and documentation about how Smithsonian Data is used, collected, maintained, stored, or shared.

[1/] [2/] Additional requirements for contracts that involve cardholder data or PCI sensitive authentication data are included in Section 6.

(b) Contractor shall make any Smithsonian Data not previously accessible to the Smithsonian, accessible to the COTR as soon as possible, but no later than ten (10) calendar days of receiving a request from the COTR. **(c)** Contractor shall transfer all Smithsonian Data to the COTR no later than thirty (30) calendar days from the date of the request from the COTR. **(d)** Unless otherwise specified in this contract, Contractor shall purge any Smithsonian Data from its files and shall provide the COTR a Certificate of Destruction confirming the purging of the Smithsonian Data within forty-five (45) calendar days of receiving a request from the COTR or at the expiry of this contract. **(e)** The Contractor shall, when required to transfer Smithsonian Data to the COTR under the terms of this contract, provide that Smithsonian Data in one or more commonly used file or database formats as the COTR deems appropriate. **(f)** The Contractor shall only be permitted to use non-Smithsonian provided information technology assets to access or maintain Smithsonian Data if Contractor provides, and the COTR approves, the following written certifications about the non-Smithsonian provided information technology assets: **(i)** The Contractor shall maintain an accurate inventory of the information technology assets. **(ii)** The Contractor shall keep all software installed on the information technology assets, especially software used to protect the security of the information technology assets, current and free of significant vulnerabilities. **(iii)** The Contractor shall encrypt all Smithsonian Data stored or accessed on a non-Smithsonian provided mobile device (e.g. phone, laptop, tablet, or removable media) using a Federal Information Processing Standards 140-2 certified encryption method. **(iv)** The Contractor shall utilize anti-viral software on all information technology assets used under this contract. **(v)** The Contractor shall encrypt all transmissions of PII using Transport Layer Security (TLS) 1.1 or higher with secure cyphers. Secure Sockets Layer (SSL) shall not be used.

4. If the Contractor uses or provides Public-Facing Software in order to carry out the requirements of this contract, the Contractor shall ensure that: (a) The Public-Facing Software and its usage comply with Smithsonian's Privacy Statement located at: http://www.si.edu/Privacy. **(b)** The Public-Facing Software and its usage comply with the Smithsonian Kids Online Privacy (SKOP) Statement located at: http://www.si.edu/privacy/kids. **c)** The Public-Facing Software provides the public with accurate privacy notices in locations that are acceptable to the Smithsonian Privacy Office. **d)** If the Contractor discovers that information was collected from someone under the age of 13 in violation of the SKOP's parental permission requirements, the Contractor shall: **(i)** Provide notice to the Smithsonian Privacy Office as soon as possible, but no later than 24 hours after discovery. **(ii)** Delete that information as soon as possible, but no later than 24 hours after discovery.

5. If the Contractor uses Public-Facing Software that employs tracking technology (such as geolocation or a cookie, web bug, or web beacon), or collects contact information, in order to carry out the requirements of this contract: (a) The Contractor shall ensure that the Public-Facing Software **(i)** Provides all users with an accessible opportunity to accept or decline ("opt-in") the use of any tracking technology, and **(ii)** Provides users who decline with reasonable access to the Public-Facing Software. **(b)** If any tracking technology uses geolocation data, the Contractor shall design the Public-Facing Software to provide an accessible opportunity for users to accept or decline the use of such data prior to use (i.e., "just in time" notice and consent), and shall disclose the use of geolocation data in the Public-Facing Software's static privacy notice. **(c)** The Contractor shall ensure that the Public-Facing Software provides all users who opt-in to the use of persistent web tracking or geolocation technology, or the receipt of communications, a subsequent and accessible opportunity to request that the tracking or communications cease ("opt-out").

6. If the Contractor collects, processes, stores, transmits, or affects the security of cardholder data or PCI sensitive authentication data, either directly or through a third party, in order to carry out the requirements of this contract: (a) The Contractor shall provide the COTR, before this contract begins and annually thereafter, a current, complete, comprehensive, and signed PCI Data Security Standard (DSS) Attestation of Compliance (AOC).[3/] **(b)** Each payment device must adhere to the current Personal Identification Number Transaction Security (PTS) standard.[4/] **(c)** Each system used to process Point of Sale card-present transactions must comply with the Smithsonian's, Office of the Chief Information Officer (OCIO) standards as provided by the COTR, to include the Technical Note IT-930-TN99, *Implementation of P2PE Devices and TransArmor Services*, or its successor. **(d)** The Contractor shall complete the *PCI DSS Requirement Management Form*, which asks whether Contractor or a third party shall be responsible for ensuring that certain key PCI DSS requirements are met. The COTR shall provide and receive the form. **(e)** The Contractor shall provide the COTR, if requested, any evidence needed to determine the PCI compliance of activities related to this contract. **(f)** The Contractor shall provide the following documents to the COTR for review and approval before the Contractor may use the following payment processing solutions in order to carry out the requirements of this contract

[3/] When this Clause was written, a template for the PCI DSS AOC was found in the PCI Security Standards Council's Document Library (https://www.pcisecuritystandards.org/document_library).

[4/] The PTS standard is maintained by the PCI Security Standards Council.

(i) A current, complete, comprehensive, and signed PCI DSS AOC for each third party vendor who processes, stores, transmits, or affects the security of cardholder data or PCI sensitive authentication data. **(ii)** The listing from the PCI SSC website's List of Validated Payment Applications for each Payment Application. **(iii)** The listing from the PCI SSC website's Approved PTS Devices list for each payment device. **(iv)** The listing from the PCI SSC website's Point-to-Point Encryption Solutions list for each system used to process Point of Sale card-present transactions. **(g)** The Contractor shall provide updated documents and listings to the COTR for review and approval before a system change results in one or more of the required documents becoming inaccurate. **(h)** The Contractor acknowledges the responsibility to secure cardholder data or PCI sensitive authentication data any time the contractor possesses or otherwise stores, processes or transmits on behalf of the Smithsonian, or to the extent that the contractor could impact the security of the Smithsonian's cardholder data environment.

7. If the Contractor develops, operates, or maintains an IT system or cloud service on behalf of the Smithsonian, the Contractor shall provide the necessary documentation, security control evidence, and other information needed to complete federal security Assessment and Authorization activities in accordance with the National Institute of Standards and Technology (NIST) Risk Management Framework: (a) For cloud solutions that have been Federal Risk and Authorization Management Program (FedRAMP) certified, Contractor shall provide FedRAMP documentation to the Smithsonian for review and shall cooperate with Smithsonian requests for clarification or further evidence. **(b)** For cloud systems which are not FedRAMP certified, and all other Contractor-hosted systems and websites, the Contractor shall complete all requested Smithsonian Assessment and Authorization documentation and shall fully cooperate with the Smithsonian's security assessment process, including providing requested security control evidence and access to interview appropriate Contractor personnel about security controls. **(c)** For Contractor custom developed (non-COTS) systems and websites to be hosted at the Smithsonian, the Contractor shall complete all requested Smithsonian Assessment and Authorization documentation for the components/aspects of the system provided by Contractor, and shall fully cooperate with the Smithsonian's security assessment process, including providing requested security control evidence and access to interview appropriate Contractor personnel about security controls. **(d)** The Contractor shall not implement into live production use any system or website operated for the Smithsonian or containing Smithsonian Data until security and privacy authorization has been granted in writing by the OCIO and the Smithsonian Privacy Officer via the COTR. **(e)** For contracts that do not require Contractor personnel to have access to Smithsonian-managed systems, the Contractor is responsible for applying industry best practice background screening, security and privacy training, and other appropriate personnel security safeguards to the services performed under this contract. The Contractor shall, if requested by the COTR, require its employees to sign a nondisclosure agreement, sign a conflict of interest agreement, and sign an acknowledgement of the requirements in this contract.

8. In the event of a Privacy Incident, Security Incident or Breach involving Smithsonian Data, the Contractor shall immediately, but no later than twenty-four (24) hours after discovery, report the Incident through the following process: (a) Contractor shall report the Privacy Incident, Security Incident, or Breach to the Smithsonian OCIO Help Desk (OCIO Help Desk) by calling 202-633-4000. If the OCIO Help Desk does not answer the telephone, Contractor shall leave a voicemail which includes, at a minimum, the name of the Contractor, a brief summary of the Incident or Breach, and a return telephone number. (**b**) If the OCIO Help Desk does not answer the telephone, Contractor shall continue to contact the OCIO Help Desk, at a minimum, three times within every 24 hour period until a representative of the OCIO Help Desk acknowledges the Privacy Incident, Security Incident, or Breach. The Contractor is not required to leave additional voicemails for the OCIO Help Desk if the information in a prior voicemail remains accurate. **(c)** The Contractor shall follow industry standard best practices to correct and mitigate any breach resulting from Contractor's access to Smithsonian Data. **(d)** The Contractor shall indemnify and hold the Smithsonian harmless from any costs incurred by the Smithsonian in connection with a Privacy Incident, Security Incident, or Breach caused in whole or part by the Contractor's failure to comply with its obligations under this contract.

9. If any of the Contractor's employees require a Smithsonian credential, network account or other access, or other Smithsonian furnished equipment in order to complete the work of this contract: (a) The Contractor shall notify the COTR at least two weeks before any employee stops supporting the work of this contract. In the event that the Contractor is not provided two weeks' notice by its employee, the Contractor will notify the COTR as soon as the Contractor becomes aware of the employee's departure from the contracted work. (**b**) The Contractor shall, when employees stop supporting the work of this contract, provide their Smithsonian credential and any Smithsonian furnished equipment to the COTR within three (3) business days.