TECHNICAL OR PROFESSIONAL, NON-PERSONAL SERVICES
WEB AND SOCIAL MEDIA ARCHIVING

This Request for Quote (RFQ) is issued by the Smithsonian Libraries & Archives (SLA), Smithsonian Institution (SI), for technical, professional, non-personal services to provide web and social media archiving services in accordance with the Statement of Work (SOW.)

I. SUBMITTING YOUR QUOTE

Price quotes may be submitted by electronic mail (email).
Quotes are due by 5 p.m (Eastern), Friday ***April 5, 2024*** **at:**

Smithsonian Institution
Smithsonian Libraries and Archives
PO Box 37012
600 Maryland Ave SW
Capital Gallery West, Suite 3000
Washington, DC 20013-7012

Attn: Lynda Schmitz Fuhrig
Fax: 202-633-5917
Email to: SchmitzfuhrigL@si.edu

You are hereby informed that mail via U.S. Postal Service to Smithsonian organizations is received at a central sorting and distribution unit and is not date stamped received until actually received and opened at the street address listed above. It is advisable that quotes and documents included as part of quote packages be emailed, hand delivered or submitted via direct package delivery companies to the street address listed above.

Any questions regarding the Request For Quote or Statement of Work should submitted by March 29, 2024 and directed by email to Lynda Schmitz Fuhrig (schmitzfuhrigl@si.edu).

II. DESCRIPTION OF REQUIRED SERVICES

The Smithsonian Institution has a requirement for Web and Social Media Archiving services at the Smithsonian Libraries and Archives, Capital Gallery in Washington, DC. A Firm-Fixed Price award to a single vendor is contemplated. This firm-fixed price shall include all direct and indirect costs necessary to complete the requirements as outlined in the SOW.

III. EVALUATION

The SI plans to award based on best value to the SI considering the following factors listed below (A-C). The SI plans to award without discussions, however, does reserve the right to conduct discussions if later determined by the Contracting Officer to be necessary.

All of the following factors are of equal importance. Evaluation factors are:

A. Price

The price evaluation will cover the pricing submitted for the base year, with no options.

B. Relevant Experience/Past Performance

1. Relevant experience is that obtained within the past three (3) years providing or performing services of similar size, scope, complexity and type of client that indicates your suitability for this project. The incumbent will provide a brief narrative summary of his/her experience in, educational training in and knowledge of the web and social media archiving skills outlined in the Statement of Work, including experience with Archive-It, Browsertrix or similar web archiving tools and applications The summary will include a minimum of two (2) and a maximum of three (3) past projects, customers, timeframes, contract dollar values, locations of performance and complexity of work to facilitate determination of capabilities to perform the work required as cited in the Statement of Work.

2. Past Performance should be indicated by a list of current or previous contracts for formal projects with the names, current email addresses and telephone numbers of points of contact who can answer specific questions of quality, workmanship and scheduling. Provide periods of performance dates, brief description of the work performed and dollar value.

3. Samples will not be accepted after the time specified for receipt of quotes. Product samples shall be submitted at no expense to the Smithsonian Institution and will be returned at the sender's request and expense, unless they are destroyed during pre-award testing.

4. The contractor to perform the work will also provide a resume highlighting education, work experience, qualifications, and technical competence that demonstrate the contractor meets the requirements of the SOW.

C. Qualifications/Technical Competence

1. **Technical Information** - Technical information should include a narrative discussion addressing the technical competence, the firm's capabilities, qualifications, and

approach to satisfy the requirements of the SOW. Technical competence must include a working knowledge of and experience working in the field of digital curation and preservation.

2. **Product Samples** - Examples of similar services' size, scope, complexity and type of client:

   Smithsonian Institution Archives Accession 17-024
   Hirshhorn Museum and Sculpture Garden
   Website Records, 2012-2016 - https://wayback.archive-it.org/3340/20160613170210/https://hirshhorn.tumblr.com/

   National Museum of African Art
   Website Records, captured 2023 - https://wayback.archive-it.org/3340/20230210161422/https:/africa.si.edu/)

D. Résumés. Résumés of potential contractor assignees may be requested.

IV. INSURANCE REQUIREMENTS

Prospective contractors are required to have *General Liability Insurance*. The SI must be listed as additional insured for the contractor's General Liability insurance or the contractor may obtain insurance through the Smithsonian Institution. Proof of insurance, or a statement on intent to obtain insurance in advance of the period of performance, must be submitted with quotes. Work may not begin without proof of insurance.

V. SYSTEM FOR AWARD MANAGEMENT (SAM) REGISTRATION

It is a requirement that current and prospective recipients of contracts and purchase orders awarded by the SI must have an active SAM registration to be eligible for awards, and maintain an active record in SAM throughout the period of time the SI award will be in effect. The SAM requires a one-time business registration, with annual updates, and allows vendors to control the accuracy of the business information they enter. The financial data you enter, which includes the electronic funds transfer (EFT) data collected by SAM, will assist the SI with correctly directing payments on your invoices and complying with the Federal Debt Collection Improvement Act of 1996.

Within thirty (30) calendar days after your SAM registration is activated you must mail a notarized letter to SAM. You will receive guidance on this procedure throughout the SAM registration process and again after your SAM registration is activated. Federal agencies, including SI, have been assured that once an entity's SAM registration is activated, agencies may engage that entity. Notarized letters from registered entities will need to contain specific language. OCon&PPM has provided the preferred language for letters with our form memo OCon 120 – Mandatory Registration in the System for Award Management (SAM) that accompanies this RFQ.

If yours is the acceptable price quote and you are selected for award, your organization's active registration with SAM must be verifiable by SI staff managing this procurement prior to contract or purchase order award being executed, and at the time any modifications or amendments to awards might be required.

You may complete or update your SAM registration information anytime online at http://sam.gov. Questions regarding the process may be directed to the Federal Service Desk online at www.fsd.gov or via toll free call to 1-888-606-8220. There is no charge for registering in SAM.

VI. UNIQUE ENTITY IDENTIFIER (UEI) NUMBER

A UEI number is a unique twelve-digit alpha-numeric identifier that will be assigned to you when your SAM registration is completed. A UEI is available for each physical location of your business (see Section V. of this RFQ). You will need to maintain your assigned UEI(s) in a safe location where they may be easily accessed. Your UEI will be required whenever you need to annually update your SAM registration or make changes to your SAM registration information at any time.

VII. LEGISLATIVE AND/OR ADMINISTRATIVE REQUIREMENTS

A. Service Contract Act of 1965, as amended

If services to be performed are covered by the Service Contract Act (SCA), as amended, the SCA shall apply to all work performed under the contract, purchase order, or GSA schedule task order to be issued. Individuals and companies submitting quotes are encouraged to verify the wages and fringe benefits determined by the U.S. Department of Labor to be payable for the Labor Category and in within the location that work performance will occur as cited in the Statement of Work. The SCA wages and fringe benefits payable shall be part of the order award.

Individuals and companies awarded a contract, purchase order or GSA schedule contract task order for SCA covered services are responsible, and required by law, to deliver to its employee(s) or post a notice of the required compensation in a prominent place at the worksite. The SCA provides authority to contracting agencies to withhold contract funds to reimburse underpaid employees, terminate the contract, hold the contractor liable for associated costs to the government, and debar from future government contracts for a period of three (3) years any persons or firms who have violated the SCA. The contracting officer awarding this order, or the Smithsonian Inspector General, may periodically require contractors to provide information that verifies compliance with the SCA for services provided under the awarded contracts, purchase orders or GSA schedule contract task orders.

B. E-Verify

If at award, or anytime during contract performance, the dollar amount of the contract award exceeds $150,000 or $5,000,000 under GSA Schedule, with a period of performance over 120 days, the successful bidder is required to register in the E-Verify System and verify that all individuals to be hired under the contract award are eligible for employment within the U.S. This requirement is not applicable to work that will be performed outside the U.S. or for Commercial Off the Shelf (COTS) items.

E-Verify is an Internet-based system operated by the Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS). It allows employers to verify the employment eligibility of their employees, regardless of citizenship. For more information on e-verify and when, why and how to register and use the system please go to the USCIS site on the World Wide Web at E-Verify.gov.

Executive Order 13465 and Homeland Security Policy Directive 12 (HSPD-12)

C. Background Investigations

If a contractor employee assigned to the SI under this contract will have an association with SI that will be greater than thirty (30) days, determined either at time of contract award or anytime during contract performance, and will need access to staff-only areas of SI controlled facilities and leased spaces, the employee shall be required to receive an SI Credential. Contractor employees who require an SI Credential shall be required to undergo and pass an appropriate background investigation and complete security awareness training before an SI Credential is issued. Employees whose associations with the SI will be less than 30 days shall not receive a background investigation or SI Credential, however, they must be escorted by Credentialed personnel at all times when in staff-only areas of SI facilities. If relevant to this RFQ, a form OCon 520, Background Investigations and Credentials for Contractors' Personnel, is included. The following actions shall be required to be completed by the SI Contracting Officer's Technical Representative (COTR) and successful vendor:

1. The COTR shall provide an OF-306, Declaration for Federal Employment form, for each of the Contractor's employees who will be assigned to the SI for 30 days or longer. The OF-306 forms must be completed by each person and returned by the Contractor to the COTR, or other designated SI employee, within ten (10) workdays from receipt of the forms by the Contractor.

2. For contractors to SI organizations outside the Washington DC and New York City areas, forms SF-87, Fingerprint Cards, shall be provided to the Contractor by the COTR or other designated SI employee. Each form SF-87 must be returned to the COTR, or other designated SI employee, within ten (10) workdays from receipt of

the forms by the Contractor When necessary, the forms SF-87 shall be submitted by the Contractor with the OF-306.

Homeland Security Policy Directive 12 (HSPD-12)

VIII. INFORMATION TO BE SUBMITTED WITH QUOTES

Quotes submitted must include the following information to be deemed responsive to this Request for Quote and accepted by the SI:

A. Documentation of your current active SAM registration with the date it will expire
B. Project Title: Web and Social Media Archiving Services
C. Business name, address, telephone number, and UEI number
D. Business point of contact name, telephone number and email address
E. Pricing. Ensure that the base period pricing is included.
F. Past Performance information should include the contract title, company/customer name, contact person with telephone number and other relevant information enumerated under the Evaluation, Relevant Experience/Past Performance section above for at least 3 recent relevant contracts for the same or similar goods and/or services.
G. Certificates or other documentation confirming appropriate types and levels of insurance required are in effect, and other certificates and documentation requested.
H. If services are subject to the requirements of the Service Contract Act provide with your quote:

1. U.S. Department of Labor wage determination hourly rate payable within the location of work performance
2. Health and Welfare hourly rate payable within the location of work performance
3. IFF hourly rate payable within the location of work performance
4. G & A hourly rate payable (e.g., markup, overhead, etc.) within the location of work performance
5. Vacation hourly rate payable within the location of work performance
6. Holiday hourly rate payable within the location of work performance

I. If requested in the RFQ, provide résumés of personnel that may be assigned to perform work under the anticipated award.
J. When prices quoted are in accordance with the terms of a General Services Administration (GSA) schedule contract, provide the following information: your GSA contract number, SIN, goods and/or services pricing.
K. Indicate any discounts to your GSA schedule contract pricing that is being extended to the SI by your price quote(s).
L. Cite the date through which pricing submitted is valid.

ATTACHMENT(S):

- Statement of Work for Web and Social Media Archiving Services, January 31, 2024.
- Form SI 147A, Smithsonian Institution Purchase Order Terms and Conditions
- Form SI 147B, Smithsonian Institution Privacy and Security Clause
- OCon 120, Mandatory Registration in the System for Award Management (SAM)
- Form SI-147A, Smithsonian Institution Purchase Order Terms and Conditions
- Form SI-147B, Smithsonian Institution Privacy and Security Clause
- Rights-In-Data Clause
- Confidentiality Clause
- OCON 520
- OCON 102, COTR Clause
- Smithsonian Directive 931, Use of Computers and Network

Quote Cover Sheet for Technical or Professional, Non-personal Services

Presented to: Smithsonian Libraries and Archives

Submitted by

Name: _____

Address: _____

_____

Email: _____

Phone: _____

For Service: Web archiving technician

Availability: ☐ Part-time or full-time for up to 960 hours (six months),

Registered in the System for Award Management (SAM): ☐ Yes / ☐ Not yet
If yes, please provide UEI & expiration date:

QUOTE: $ per hour:

Signature: _____

Date:_____

Smithsonian
Libraries and Archives

Statement of Work

January 31, 2024

Smithsonian Libraries and Archives
Web and Social Media Archiving Technician

BACKGROUND

The Smithsonian Libraries and Archives (SLA) serves researchers worldwide with its specialized collections, research data and primary source material. SLA- Archives documents the Smithsonian's history from its inception in 1846 to today.

The SLA Digital Curation Program has been preserving and providing access to the Institution's digital history as captured in born-digital objects and records dating back over four decades. One very important aspect of the Smithsonian's mandate to acquire and disseminate knowledge is its use of the Internet, specifically websites, web applications and social media platforms.

With its early online presence, the Smithsonian Astrophysical Observatory launched its Telescope Data Center website in 1993, which was one of the first 250 websites on the Internet. Joining the World Wide Web continued with the Smithsonian Institution premiering its first main homepage in 1995. SLA recognized the importance of this far-reaching technology in documenting the Institution's rich history and started various web archiving initiatives that continue today through its digital curation program. SLA seeks a 6-month contractor to assist with these web archiving preservation efforts.

PROJECT DESCRIPTION

SLA seeks services of a web and social media archiving technician for the following:

- conducting crawls of Smithsonian websites and social media accounts with tools including, but not limited, to Archive-It and Browsertrix for a period of 960 hours, the equivalent of six (6) months.
- updating metadata and various internal database/spreadsheet entries
- downloading and packaging website crawls for accessioning
- performing quality assurance of crawls
- reconciling legacy website records in native formats for accessioning
- troubleshooting issues with digital archivist and others on digital curation team
- submitting written progress reports and meeting with SLA staff to inspect work, discuss issues, and present progress

TIMELINE

Smithsonian Libraries and Archives
Smithsonian Institution Archives
Capital Gallery, Suite 3000
PO Box 37012 MRC 507
Washington, D.C. 20013-7012

Smithsonian
Libraries and Archives

The contract will begin on or about May 1, 2024. All final services and deliverables shall be delivered and completed no later than November 1, 2024.

WORK LOCATION

All work performed under this contract will take place remotely with the opportunity for occasional on-site attendance if possible. Contractor must supply their own computer equipment to perform this work and agrees to follow Smithsonian Institution security procedures. Work typically takes place during normal working hours Monday through Friday, excluding federal holidays. Contractor agrees to be available for virtual meetings and check-ins through Microsoft Teams and Zoom.

PRICE

This is a firm-fixed hourly price purchase order, that should be based on 40 hours per week and shall include all costs. No overtime or holiday work is necessary to complete these services.

PAYMENT SCHEDULE

Payments shall be made upon completion and acceptance of interim and final deliverables and services listed above for the processing of and receipt of proper invoices referencing the purchase order number assigned.

Payments upon invoice for each 160-hour period worked.

DELIVERABLES

Successfully capture, preserve and verify websites and social media accounts as directed by the project COTR.

Submit monthly progress reports to the COTR to include reporting period, hours worked, and descriptive summary of all the work performed during the reporting period.

Deliverable Expectations:

Month 1	Start of web crawling/captures, metadata entry, quality assurance, downloading and packaging.
Month 2	Complete assigned web crawling/captures. Continue metadata entry, quality assurance, downloading and packaging.
Month 3	Complete assigned web crawling/captures. Continue metadata entry, quality assurance, downloading, and packaging.
Month 4	Complete assigned web crawling/captures. Continue metadata entry, quality assurance, downloading and packaging.

Month 5	Continue web archival work. Start reconciliation of legacy website records
Month 6	Continue web archival work and reconciliation of legacy website records
Months 1-6	Prepare and submit monthly status reports on progress. Meet with team on regular basis

9. INSPECTION AND ACCEPTANCE

Acceptance will be based on the following criteria and to the Smithsonian's satisfaction. All deliverables shall be delivered to SI on time according to the agreed upon schedule.

1. All deliverables shall require Smithsonian approval and acceptance. Deliverables will be approved, accepted or rejected by the COTR.

2. All deliverables shall be of an acceptable quality addressing the requirements clearly and professionally.

3. If the draft deliverable is adequate, the Smithsonian will accept the draft and provide comments for incorporation into the final version. All of the SI's comments to deliverables must either be incorporated in the succeeding version or the contractor must demonstrate to SI's satisfaction why such comments could not be incorporated.

4. If the draft deliverable is not adequate, the Smithsonian will reject the draft with a general explanation of the deficiencies. The Smithsonian will not reimburse such corrections.

5. Deliverables, both hardcopy and electronic, will be accepted when all discrepancies, errors, or other deficiencies have been resolved to the Smithsonian's satisfaction.

6. All notifications of rejection will be accompanied by specific justification or substantiation of the reason(s) for rejection.

Acceptance:

The contractor shall complete deliverables by the time schedule established by this Statement of Work. The contractor shall communicate in a professional and timely manner with all SLA staff and affiliated personnel.

CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (COTR)

Lynda Schmitz Fuhrig, Digital Archivist, will serve as Contracting Officer's Technical Representative (COTR) and project manager. Contact information for the COTR can be found in the text of the purchase order.

SPECIAL REQUIREMENTS

The following are required:

- The contractor will have at least one year of using web archiving technologies as demonstrated from past work experiences, training, and/or schooling.
    - Please provide examples of previous web archiving efforts.
    - Web archiving references desired.

The following special requirements shall be followed specifically as cited and as general guidance for production of this work.

- Smithsonian policies
    - Anti-Harassment Policy (https://www.si.edu/sites/default/files/unit/ohr/sd_225_anti-harassment_policy_12-30-2020.pdf)
    - The Smithsonian embraces diversity and equal employment opportunity (www.si.edu/oeema).
    - Use of Computers, Telecommunication Devices, and Networks (https://lweb.cfa.harvard.edu/cf/forms/public/sd931.pdf)

SMITHSONIAN INSTITUTION
PURCHASE ORDER TERMS AND CONDITIONS

1. COMPLETE AGREEMENT - The purchase order and all documents attached represent the entire agreement between the Smithsonian Institution (SI) and the Contractor. Any modification, alteration or amendment to this purchase order must be in writing and signed by an authorized agent of the SI.

2. INSPECTION AND ACCEPTANCE - The Contractor shall tender for acceptance only those items that conform to the requirements of this contract. The SI reserves the right to inspect, test or evaluate any supplies or services that have been tendered for acceptance. The SI may require repair or replacement of nonconforming supplies or re-performances of nonconforming services at the Contractors expense. The SI must exercise its post acceptance rights- **(a)** Within a reasonable period of time after the defect was discovered or should have been discovered; and **(b)** Before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item. Inspection and acceptance will be at destination, unless otherwise provided in writing. Until delivery and acceptance, and after any rejections, risk of loss will be on the Contractor unless loss results from negligence of the SI. Final acceptance by the SI will be conditional upon fulfillment of the above requirements.

3. OVERPAYMENT - If the Contractor becomes aware of a duplicate invoice payment or that the SI has otherwise overpaid on an invoice payment, the Contractor shall immediately notify the Contracting Officer and request instructions for disposition of the overpayment.

4. USE OF SMITHSONIAN NAME or LOGO PROHIBITED - The SI owns, controls and/or has registered the trademarks /service marks "Smithsonian," "Smithsonian Institution" and the Smithsonian sunburst logo. Except as may be otherwise provided herein, the Contractor shall not refer to the SI or to any of its museums, organizations, or facilities in any manner or through any medium, whether written, oral, or visual, for any purpose whatsoever, including, but not limited to, advertising, marketing, promotion, publicity, or solicitation without written consent.

5. WARRANTY - The Contractor warrants and implies that the goods and services furnished hereunder are merchantable, fully conform to the SI's specifications, drawings, designs, and are fit for intended use described in this contract. The Contractor agrees that the supplies or services furnished under this contract shall be covered by the most favorable commercial warranties the Contractor gives to all customers for such supplies or services, and that the rights and remedies provided herein are in addition to and do not limit any rights afforded to the Government by any other clause of this contract. Contractor agrees to pass through all warranties from other manufacturers.

6. TITLE - Unless otherwise specified in this contract, title to items furnished under this contract shall pass to the SI upon acceptance, regardless of when or where the SI takes physical possession.

7. EXCUSABLE DELAYS - The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence, such as acts of God or the public enemy, acts of the SI, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

8. DISPUTES - Any dispute arising under this contract that the parties are unable to resolve shall be decided by the Contracting Officer. All disputes must be submitted to the Contracting Officer in the form of a written claim supported by evidence within twelve (12) months following accrual of the claim. The Contracting Officer will provide a written decision to the Contractor, and that decision is the final and conclusive decision of the Smithsonian Institution, which is effective on the date the Contractor receives the decision. The Contractor retains all rights to subsequent judicial review to which it is entitled under federal law. The Contractor shall comply with any decision of the Contracting Officer and otherwise proceed diligently with performance of this contract pending final resolution of any request for relief, claim, or action arising under the contract.

9. TERMINATION FOR CAUSE - The SI may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the SI, upon request, with adequate assurances of future performance. In the event of termination for cause, the SI shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the SI for any and all rights and remedies provided by law. If it is determined that the SI improperly terminated this contract for default, such termination shall be deemed a termination for convenience.

10. TERMINATION FOR THE SMITHSONIAN'S CONVENIENCE - The SI reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid a percentage of the contract price reflecting the percentage of the work performed prior to the notice of termination, plus reasonable charges that the Contractor can demonstrate to the satisfaction of the SI, using its standard record keeping system, have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the SI any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred that reasonably could have been avoided.

11. CHANGES - The SI may at any time, in writing, make changes within the general scope of this purchase order to include. **(a)** Technical requirements and descriptions, specifications, statements of work, drawings or designs; **(b)** Shipment or packing methods; **(c)** Place of delivery, inspection or acceptance; **(d**) Reasonable adjustments in quantities or delivery schedules or both; and, **(e)** SI-furnished property, if any. If any such change causes an increase or decrease in the cost of or the time required for performance of this purchase order, the Contractor shall inform the SI in writing within thirty (30) days after receipt of change request. Any additional charges must be approved in writing by the SI authorized procurement officer executing this purchase order. Contractor shall not make any changes without the written consent of the SI authority executing this purchase order.

12. CONFIDENTIALITY and DISCLOSURE - Confidential Information. Confidential Information consists of trade secrets, product concepts, customer information, marketing communication material, marketing strategies, and other commercial or financial information that if affirmatively used by a competitor of the disclosing party would cause the disclosing party substantial competitive harm or information the release of which would violate the privacy rights of a third party with no overriding public interest. If Confidential Information is disclosed in tangible form, it shall be

clearly designated in writing as such by the disclosing party. If Confidential Information is disclosed other than in writing, the information deemed to be Confidential Information shall be confirmed in writing as such within thirty days of such disclosure.
Limited Disclosure -- Each party agrees that it will not disclose Confidential Information provided to it by the other party to others except to the extent that it is necessary to disclose such Confidential Information to its directors, officers, representatives, legal and financial consultants, and employees having a need to know such Confidential Information ("authorized parties") for the purpose of pursuing a business and contractual relationship between the parties. The parties shall use at least the same degree of care that each party uses to protect its own Confidential Information of similar importance, but no less than a reasonable degree of care. Further, the parties may disclose Confidential Information if required by law, subpoena, order or request of a federal governmental authority or court of competent jurisdiction, and further, provided that the party obligated to disclose such Confidential Information shall **(a)** assert the confidential nature of the Confidential Information to be disclosed, **(b)** use reasonable efforts to obtain confidential treatment for any Confidential Information so disclosed, and **(c)** immediately notify the other party of the requirement, order, or request to disclose in advance of such disclosure in order to afford the other party the opportunity to contest disclosure. No other use or disclosure of Confidential Information may be made by any party without the prior written consent of the disclosing party.
13. INDEMNITY - The Contractor shall defend, indemnify, and hold harmless the SI, its Regents, directors, officers, employees, volunteers, licensees, representatives, agents and the United States Government (hereinafter referred to as "Indemnitees") from and against all actions, causes of action, losses, liabilities, damages, suits, judgments, liens, awards, claims, expenses and costs including without limitation costs of litigation and counsel fees related thereto, or incident to establishing the right to indemnification, arising out of or in any way related to:

Any breach of this Agreement, Terms and Conditions, and the performance thereof by Contractor, Subcontractor, other third parties, or any activities of Indemnitees, including, without limitation, the provision of services, personnel, facilities, equipment, support, supervision, or review; any claims of any kind and nature whatsoever for property damage, personal injury, illness or death (including, without limitation, injury to, or death of employees or agents of Contractor or any Subcontractor).

Any claims by a third party of actual or alleged direct or contributory infringement, or inducement to infringe any United States or foreign patent, trademark, copyright, common law literary rights, right of privacy or publicity, arising out of the creation, delivery, publication or use of any data furnished under this contract or any libelous or other unlawful matter contained in such data or other intellectual property rights and damages. The contractor shall notify the SI immediately upon receiving any notice or claim related to this contract.
14. HAZARDOUS MATERIAL - The Contractor shall inform the SI in writing at the correspondence address listed on the purchase order prior to shipment and delivery of any hazardous material. Any materials required by this purchase order that are hazardous under federal, state or local statute, ordinance, regulation, or agency order shall be packaged, labeled, marked and shipped by the Contractor to comply with all federal, state and local regulations then in effect.
15. OTHER COMPLIANCES - The Contractor shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract.
16. SECURITY CONSIDERATION - OPS, OCon 520 Contractor's conducting work on the SI premises are required to obtain a temporary or long-term identification badge. Contractor's employee (s) requiring a long-term identification badge is subject to a fingerprint review. An adverse finding during the fingerprint review may prohibit a contractor's employee (s) from working on the contract. The SI will inform the contractor if a long-term identification badge is required.
17. **INSURANCE and BONDS** - Contractor shall maintain at all times during the performance of this contract Commercial General Liability Insurance. Contractor shall maintain Worker's Compensation Insurance in accordance with statutory requirements and limits. If during the performance of this contract, a vehicle is required, contractor shall maintain business automobile insurance. If this contract relates to any type of media exposure, then Contractor is required to have professional errors and omissions coverage. If this contract requires Contractor to handle Smithsonian funds or guard or protect Smithsonian artifacts, Contractor will also be required to obtain a fidelity bond or crime insurance. Limits of such bonds or insurance policies are to be determined. SI shall be listed as an "additional insured" under the comprehensive general liability and business automobile policies. Proof of insurance shall be in the form of a binder, policy, or certificate of insurance and this is to be submitted to the SI's Procurement Officer prior to work being initiated.
18. INVOICE INSTRUCTIONS - Invoices shall be submitted to the bill to address on the face of the purchase order after delivery of supplies and/ or services, and shall contain the following information: **(a)** Contractor's name, address, and taxpayer identification number (TIN). **(b)** Invoice date and number. **(c)** Purchase order number including contract line item number. **(d)** Item description, quantity, unit of measure, unit price, and extended price. **(e)** Name, title, telephone and fax number, and mailing address of point of contact in the event of an invoice discrepancy. **(f)** Invoice total, payment discount terms and remittance address. **(g)** Shipping and payment terms (e.g. shipment number, date of shipment, and discount terms). Bill of lading number and weight of shipment should be included when using Smithsonian Institution bills of lading. Prepaid shipping costs shall be indicated as a separate item on the invoice. **(h)** Any other information or documentation required by other provisions of the contract.
19. Travel - (a) If travel is specified under this purchase order; it must be pre-authorized by the Contracting Officer's Technical representative (COTR) prior to occurrence. The Contractor shall be reimbursed for such travel upon receipt of documentation that the expenses were incurred. **(b)** Rail or air transportation costs shall not be reimbursed in an amount greater than the cost of economy class rail or air travel unless the economy rates are not available and the Contractor certified to this fact in vouchers or other documents submitted for reimbursement. **(c)** Room and meals (per diem travel allowance) shall be reimbursed in accordance with the Contractor's established policy, but in no event shall such allowances exceed the rates Contractor's established in the Federal Travel Regulations. **(d)** The contractor shall be reimbursed for the cost of the out-of-town travel performed by its personnel in their privately owned automobiles at the rates established in the Federal travel Regulations, not to exceed the cost by the most direct economy air route between the points so traveled. If more than one person travels in the same automobile, the Contractor for such travel shall incur no duplication of or otherwise additional charges. **(e)** The Contractor shall be reimbursed upon receipt of appropriate documentation that the expenses were incurred. Total travel cost will not be reimbursed for an amount that exceeds the estimated amount stated in this purchase order.
20. RESPONSIBILITY OF SMITHSONIAN PROPERTY - Contractor assumes full responsibility for and shall reimburse and indemnify the SI for any and all loss or damage whatsoever kind and nature to any and all **SI property,** including any equipment, supplies, accessories, or parts furnished, while in the Contractor's custody and care, or resulting in whole or in part from the negligent acts, omissions of the Contractor, any subcontractor, or any employee, agent, or representative of the Contractor or subcontractor.

21. INTERNET PROTOCOL VERSION 6 (IPV6) COMPLIANCE - In the event that the Contractor will be developing, acquiring, and/or producing products and/or systems pursuant to this Contract that will be connected to a network or that will interface with the World Wide Web, the following provisions shall apply: OMB Memo M-05-22, dated August 2, 2005, and OMB guidance, dated July 2012 September 28, 2010, that requires procurements of networked IT comply with the USGv6 Profile and Test Program for the completeness and quality of SI IPv6 capabilities. The Contractor hereby warrants and represents that such products and/or systems to be developed, acquired, and/or produced pursuant to this Contract will be IPv6 compliant. These products and/or systems must be able to receive, process, and transmit or forward (as appropriate) IPv6 packets and must be able to interoperate with other systems and protocols in both IPv4 and IPv6 modes of operation. If the product or system will not be IPv6 compliant initially, the Contractor will provide a migration path and express commitment to upgrade to IPv6 for all application and product features. Any such migration path and commitment shall be included in the Contract price. In addition, the Contractor will have available contractor/vendor IPv6 technical support for development and implementation and fielded product management.

CLAUSES INCORPORATED BY REFERENCE -This contract incorporates one or more clauses by reference with the same force and effect as if they were given in full text. The applicability of these clauses is effective upon the date of the actual contract award. Upon request the Contracting Official will make the full text available. The full text of the following FAR clauses may be viewed at the Federal Acquisition Regulation (FAR) website. For the full text of Smithsonian Institution clauses contact the procurement official. The Contractor shall comply with the FAR clauses incorporated by reference, unless the circumstances do not apply: References herein to the "Government" shall be deemed to mean the Smithsonian Institution.

SMITHSONIAN Clauses

- Minimum Insurance
- Smithsonian Institution Privacy and Security Clause (form SI 147B, SI Privacy and Security Clause)

FAR Clauses

- 52.222-3 Convict Labor
- 52.222-19 Child Labor - Cooperation with Authorities and Remedies
- 52.222-20 Contracts for Materials, Supplies, Articles, and Equipment Exceeding $15,000
- 52.222-21 Prohibition of Segregated Facilities
- 52.222-26 Equal Opportunity
- 52.222-35 Equal Opportunity for Veterans
- 52.222-36 Equal Opportunity for Workers with Disabilities
- 52.222-41 Service Contract Labor Standards
- 52.222-50 Combating Trafficking in Persons. (non-commercial services awards that do not exceed $500,000)
- 52.222-56 Certification Regarding Trafficking In Persons Compliance Plan (when applicable)
- 52.223-1 thru 4 Bio-based ProductCertification/Affirmative Procurement of Biobased Products Under Service and Construction Contracts/Hazardous Material Identification and Material Safety Data/Recovered Material Certification
- 52.223-5 Pollution Prevention and Right-to-Know Information
- 52.224-1 Privacy Act Notification
- 52.225-1 Buy American Supplies
- 52.225-13 Restrictions on Certain Foreign Purchases
- 52.232-11 Extras
- 52.239-1 Privacy or Security Safeguards (see form SI 147B)
- 52.233-3 Protest After Award
- 52.244-6 Subcontracts for Commercial Items

Additional FAR clauses that apply when applicable:

- 52.204-6 Universal Numbering System (DUNS) NumberUnique Entity Identifier
- 52.204-7 System for Award Management
- 52.208-4 Vehicle Lease Payments
- 52.208-5 Condition of Leased Vehicle
- 52.208-6 Marking of Leased Vehicles
- 52.208-7 Tagging of Leased Vehicle
- 52.211-6 Brand Name or Equal
- 52.211-17 Delivery of Excess Quantities
- 52.222-54 Employment Eligibility Verification (E-Verify)
- 52.228-8 Liability and Insurance Leased Motor Vehicles
- 52-233-4 Applicable Law for Breach of Contract Claim
- 52.236-5 Material and Workmanship
- 52.247-29 F.o.b. Origin
- 52.247-34 F.o.b. Destination

Smithsonian Institution
Privacy and Security Clause

1. Smithsonian Data: (a) The Smithsonian Institution ("Smithsonian") retains sole ownership of, and unrestricted rights to, any and all physical or electronic information collected, processed, or stored by or on behalf of the Smithsonian ("Smithsonian Data"), which is defined to include personal information, also referred to as personally identifiable information (PII), *i.e.*, information about individuals, which may or may not be publicly 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, online identifiers such as IP address, device IDs, and cookie data, and any other information defined as "personal information," "personal data" (or other analogous variations of such terms) under the applicable privacy, security and data protection laws ("PII"). (b) Contractor shall maintain, transmit, and retain in strictest confidence, and prevent the unauthorized duplication, use and disclosure of Smithsonian Data. (i) Contractor shall only access, maintain, use, and disclose Smithsonian Data to the extent necessary to carry out the requirements of this contract, and shall not use Smithsonian Data for any other purposes, including testing or training purposes. (ii) 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. (iii) Contractor shall ensure that all Smithsonian Data is protected from unauthorized access, disclosure, modification, theft, loss, and destruction. (iv) 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, 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. (v) 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. (c) 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 with the requirements in this contract. Contractor shall, as requested by the COTR, complete, or assist Smithsonian staff with the completion of, a privacy and/or security review which might include providing requested information and documentation about how Smithsonian Data is used, collected, maintained, stored, or shared. (d) Contractor shall make any Smithsonian Data accessible to the COTR as soon as possible, but no later than ten calendar days of receiving a request from the COTR, and shall transfer all Smithsonian Data to the COTR no later than thirty calendar days from the date of such request from the COTR. 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. (e) 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 calendar days of receiving a request from the COTR or at the expiry of this contract. (f) Contractor shall only be permitted to use non-Smithsonian provided information technology resources to access or maintain Smithsonian Data if Contractor provides, and the COTR approves, the following written certifications about the non-Smithsonian provided information technology resources: (i) Contractor shall maintain an accurate inventory of the information technology resources; (ii) Contractor shall keep all software installed on the information technology resources, especially software used to protect the security of the information technology resources, current and free of significant vulnerabilities; (iii) 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)Contractor shall utilize anti-viral software on all non-SI information technology resources used under this contract; and (v) Contractor shall encrypt all transmissions of PII using Transport Layer Security 1.2 or higher with secure cyphers. Secure Sockets Layer shall not be used. (g) Unless more substantial requirements are provided for herein, Contractor is responsible for, at a minimum, applying industry best practice background screening, security and privacy training, and other appropriate personnel security safeguards to the services performed under this contract. (h) Contractor shall, if requested by the COTR, require its employees to sign a nondisclosure agreement, sign a conflict of interest agreement, and/or sign an acknowledgement of the requirements in this contract.

2. Privacy Breach or IT Security Incident: In the event of (i) any action that threatens or is likely to threaten the confidentiality, integrity, or availability of Smithsonian IT resources (including computer hardware and software, data, communication links, mobile devices, digitized assets, automated processes, physical computing environments, and associated personnel, whether located inside or outside of the Smithsonian); (ii) any activity that violates Smithsonian IT Security policies provided by the COTR; (iii) any suspected or confirmed loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or situation where persons other than authorized users or for an

other than authorized purpose have access or potential access to Smithsonian Data or PII in a usable form, whether physical or electronic; or (iv) any suspected loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or situation where persons other than authorized users or for an other than authorized purpose have access or potential access to PII in a usable form, whether physical or electronic (collectively, "Incident"), Contractor shall: (a) Immediately, but no later than twenty- four hours after discovery, report the Incident to the Smithsonian Office of the Chief Information Officer ("OCIO") Help Desk by calling 202-633-4000 and, if the OCIO Help Desk does not answer the telephone, leaving a voicemail which includes the name of Contractor, a brief summary of the Incident, and a return telephone number; (b) The Contractor shall cooperate with Smithsonian investigations and response activities for breaches or incidents that include the Contractor's IT resources or personnel. (c) Follow industry standard best practices to correct and mitigate any damages resulting from the Incident; and (d) Indemnify and hold the Smithsonian harmless from any costs incurred by the Smithsonian in connection with such Incident.

3. Public-Facing Software: (a) Any application, system, software, or website used to fulfill the terms of this contract, which can be accessed by members of the public ("Public-Facing Software") shall comply with Smithsonian's Privacy Statement (located at Smithsonian Institution's Privacy Statement | Smithsonian Institution (si.edu) and the Smithsonian Kids Online Privacy ("SKOP") Statement (located at http://www.si.edu/privacy/kids), and such Public-Facing Software shall provide the public with privacy notices in locations that are acceptable in accordance with these policies. (b) For kiosks and interactives developed by Contractor, the Contractor shall take all reasonably necessary steps to ensure they will be maintained with antivirus software and routine patching. (c) If Contractor discovers that information was collected from someone under the age of 13 in violation of the SKOP's parental permission requirements, Contractor shall provide notice to the Smithsonian Privacy Office as soon as possible, but no later than 24 hours after discovery, and delete that information as soon as possible, but no later than 24 hours after discovery. (d) Any Public-Facing Software that employs tracking technology (such as a cookie, pixel, web bug, or web beacon) or collects contact information shall provide all users with legally-compliant notice of its data collection and tracking practices, and any required consumer choices (including the opportunity to opt-in or opt-out, as required). as well as: (i) for those who opt-out or decline the "opt-in," reasonable access to the Public-Facing Software; and (ii) for those who "opt-in", a subsequent and accessible opportunity to request that the tracking or communications cease (*i.e.*, "opt-out").

4. Cardholder Data and PCI Sensitive Authentication Data: (a) Any Contractor that collects, processes, stores, transmits, or affects the security of cardholder data or Payment Card Industry ("PCI") sensitive authentication data, either directly or through a third party, in order to carry out the requirements of this contract shall provide the COTR: (i) before this contract begins and annually thereafter, for Contractor and for any third party vendor that processes, stores, transmits, or affects the security of cardholder data or PCI sensitive authentication data, a current, complete, comprehensive, and signed PCI Data Security Standard ("DSS") Attestation of Compliance (AOC), a template for which may be accessible in the online document library of the PCI Security Standards Council ("SSC"); (ii) the *PCI DSS Requirement Management Form* provided by the COTR, which asks whether Contractor or a third party shall be responsible for ensuring that certain key DSS requirements are met; (iii) for each Payment Application, *i.e.*, application, system, software, or website used to electronically process, store, or transmit cardholder data or PCI sensitive authentication data as defined by the SSC, the listing from the SSC website's List of Validated Payment Applications; (iv) for each payment device, the listing from the SSC website's Approved Personal Identification Number Transaction Security ("PTS") Devices list; (v) for each system used to process Point of Sale card-present transactions, the listing from the SSC website's Point-to-Point Encryption Solutions list; and (vi) if requested, any additional evidence needed to determine the PCI compliance of activities related to this contract. (b) All credit card-present transactions at the Smithsonian must be processed through a PCI SSC P2PE solution and be EMV compatible. (c) Contractor shall provide the documents and listings identified in Paragraph 4(a) before it shall be permitted to use the relevant technology, and 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 or listings becoming inaccurate. (d) Each payment device that collects, processes, stores, transmits, or affects the security of cardholder data or PCI sensitive authentication data, either directly or through a third party, must adhere to the current PTS standard maintained by the SSC.(e) Each system used to process Point of Sale card-present transactions must comply with the Smithsonian Office of the Chief Information Officer ("OCIO") standards provided by the COTR, to include the Technical Note IT-930-TN99, *Implementation of P2PE Devices and TransArmor Services*, or its successor. (f) Contractor shall be responsible for securing cardholder data or PCI sensitive authentication data any time Contractor possesses or otherwise stores, processes or transmits on behalf of the Smithsonian, or to the extent that Contractor could impact the security of the Smithsonian's cardholder data environment, *i.e.*, the people, processes and technologies that store, process, or transmit cardholder data or PCI sensitive authentication data by, or on behalf of, the Smithsonian. (g)

Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they can impact the security of the customer's cardholder data environment.

5. IT Systems and Cloud Services: (a) For any Cloud System (i.e., computing service provided on-demand via a shared pool of configurable resources instead of via separate dedicated computing resources or information technology system) Contractor develops, operates, or maintains on behalf of the Smithsonian, 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 Risk Management Framework. (b) For Cloud Systems 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. (c) For Cloud Systems which are not FedRAMP certified, and all other Contractor-hosted systems and websites, 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. (d) For websites or web servers hosted outside of the Smithsonian Herndon Data Center, the Contractor must allow OCIO to perform vulnerability scanning and penetration testing. Website owners should consult with information technology security staff to determine specific needs for their environment. (e) The Contractor shall maintain all Smithsonian Data inside the United States. (f) For Contractor custom developed (non- COTS) systems and websites to be hosted at the Smithsonian, 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. (g) For Contractor developed applications or Contractor built interactive systems (e.g., public-facing exhibit technology incorporated through digital signage, custom interactives, content players, media players, audio streaming devices, lighting or control automation systems), Contractor shall not circumvent the security of system (e.g., the use of backdoor or maintenance hook provisions are prohibited). (h) Contractor shall not implement into live production or 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 Smithsonian Office of the Chief Information Officer ("OCIO") and the Smithsonian Privacy Officer via the COTR. Contractor will resolve security deficiencies in order to successfully meet the applicable requirements of this section.

6. Credentials and Network Access: (a) Contractor and Contractor's employees who have access to Smithsonian network/systems shall, when requested by the COTR, complete Smithsonian-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 Smithsonian background check, and/or provide notice of 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 networks/systems. (b) Contractor shall notify the COTR at least two weeks before any of Contractor's employee requiring a Smithsonian credential, network account or other access, or other Smithsonian-furnished equipment stops supporting the work of this contract. In the event that Contractor is not provided two weeks' notice by its employee, Contractor will notify the COTR as soon as Contractor becomes aware of the employee's departure from the contracted work. (c) Contractor shall, when any employee requiring a Smithsonian credential, network account or other access, or other Smithsonian furnished equipment stop supporting the work of this contract, provide such employee's Smithsonian credential and any Smithsonian furnished equipment to the COTR within three business days.

7. California Consumer Privacy Act: (a) The California Consumer Privacy Act, including any regulations and amendments implemented thereto ("**CCPA**") shall apply to any information collected from California residents on behalf of the Smithsonian. (b) For purposes of the CCPA, Contractor shall be considered a service provider and the Smithsonian is a business. (c) Contractor shall not collect, maintain, store, use, disclose, or share PII for a commercial purpose other than providing the services or performing its obligations to the Smithsonian. (d) Without limiting the foregoing, Contractor: (i) will not sell PII (as "sell" or "sale" is defined by the CCPA); (ii) will not retain, use, or disclose Personal Information outside of the direct business relationship between Contractor and the Smithsonian; and (iii) certifies that it understands the restrictions in this section and will comply with them. (e) Upon request by the Smithsonian, Contractor will assist the Smithsonian in the Smithsonian's fulfillment of any individual's request to access, delete, or correct PII. (f) Contractor will promptly notify the Smithsonian following Contractor's receipt of any request or complaint relating to any PII (unless applicable law prohibits such notification). Contractor will not respond to any such request or complaint, other than to redirect to the Smithsonian, unless expressly authorized to respond by the Smithsonian.

8. European Economic Area. This contract does not include the collection or processing of Personal Information relating to individuals located in the European Economic Area.

9. Terms: The bolded headings at the start of each section of this Smithsonian Institution Privacy and Security Clause are included only to assist the reader in navigating this Smithsonian Institution Privacy and Security Clause. The Parties intend the bolded headings to have no legal effect, and agree that the bolded headings are not intended to limit or modify any other language in this Smithsonian Institution Privacy and Security Clause.

SMITHSONIAN INSTITUTION
RIGHTS-IN-DATA CLAUSE

As used herein, the term "Subject Data" includes, but is not limited to, literary works; musical works, including any accompanying words; dramatic works, including any accompanying music; pantomimes and choreographic works; pictorial, graphic and sculptural works; motion pictures and other audiovisual works; sound recordings; and architectural works, as each of those terms are used and defined by the Copyright Act of the United States (17 USCS §101, et. seq.) (the "Copyright Act") and works of any similar nature (whether or not copyrighted) which are included in the material to be delivered under this contract.

(a) Work for Hire. All Subject Data first produced, composed, or created in the performance of this contract, where such Subject Data consists of a work: (i) specially ordered or commissioned for use as a contribution to a collective work; (ii) as part of a motion picture or other audiovisual work; (iii) as a translation; (iv) as a supplementary work; (v) as a compilation; (vi) as an instructional text; (vii) as a test; (viii) as answer material for a test; or (ix) as an atlas, as each of those terms are used and defined by the Copyright Act, shall be considered a "work made for hire," as that term is defined under the Copyright Act. The copyright to such Subject Data shall be the exclusive property of Smithsonian and may be registered by the Smithsonian Institution in its own name.

(b) Other Copyrightable Works. All Subject Data first produced in the performance of this contract, where such Subject Data consists of copyrightable materials that do not fall within the enumerated categories for work for hire, shall become the property of Smithsonian. Contractor hereby transfers to Smithsonian full legal title and all right, title, and interest in the copyright to all such Subject Data, including without limitation, all preliminary renditions of the Subject Data whether or not such renditions are actually delivered to Smithsonian. The copyright to such Subject Data shall be the exclusive property of Smithsonian and may be registered by the Smithsonian Institution in its own name.

(c) Except as specified herein, no Subject Data first produced in the performance of this Agreement may be published or reproduced by Contractor in whole or in part, in any manner or form, without Smithsonian's prior written consent. Contractor agrees that no right at common law or in equity shall be asserted, and no claim to copyright by statute shall be established by Contractor in any such Subject Data without Smithsonian's prior written consent. Contractor shall secure Smithsonian's legal title and interests in and to all Subject Data that is produced for Contractor by third parties pursuant to this Agreement.

(d) License for Other Subject Data. Excluding the Subject Data which Smithsonian owns or has already obtained a license for, Contractor hereby grants to Smithsonian a royalty-free, non-exclusive, perpetual, and irrevocable license in all copyrighted or copyrightable Subject Data not first produced, composed, or created in the performance of this Agreement, but which is incorporated in the material furnished under this Agreement. Such license includes, without limitation, the rights to reproduce, publish, translate, broadcast, transmit, distribute, exploit, display, use, sell, and/or dispose of such Subject Data in any manner, and to authorize others to do so. In the event that Contractor does not have the right to grant such a license with respect to any such Subject Data, Contractor shall immediately notify the Smithsonian of this fact and

obtain Smithsonian's prior written permission to incorporate such Subject Data in the work. Without this notification, Smithsonian will be acting in reliance on this contract and will presume that it possesses all necessary rights and is free to make whatever use of the Subject Data that Smithsonian determines is in its best interests.

(e) The Contractor hereby warrants that the Subject Data delivered to Smithsonian pursuant to this contract does not infringe statutory copyrights or common law literary rights of Contractor or others and contains no matter libelous or otherwise unlawful. Contractor agrees to indemnify the Smithsonian Institution, its Board of Regents, officers, agents, and employees against any liability, including costs and expenses, for: (i) violations of copyright or any other property rights arising out of the use, reproduction, or disposition of any Subject Data furnished under this contract; or (ii) based upon any libelous or other unlawful matter contained in said Subject Data.

(f) The Contractor agrees to report in writing to the Smithsonian Office of the General Counsel, promptly and in reasonable detail, any notice or claims of copyright infringement received by Contractor with respect to any Subject Data or other material delivered under this contract.

SMITHSONIAN CONFIDENTIALITY CLAUSE

CONFIDENTIALITY. The Contractor agrees that all files, records, documents, reports, donor and sponsor lists, financial data, business data, specifications, business plans and other similar or dissimilar items relating to any Smithsonian operation, department, or museum (i) provided to the Contractor by the Smithsonian; (ii) provided to the Contractor by other Smithsonian contractors; or (iii) prepared by the Contractor in performing the work, constitute "Confidential Information." The Contractor shall not use Confidential Information for any purpose other than considering or carrying out this project. No Confidential Information shall be disclosed to any person/entity without the prior written consent of the Smithsonian's Contracting Officer. Upon completion of work and/or at the request of the Smithsonian, the Contractor shall take reasonable steps to protect such Confidential Information from dissemination as would be reasonably likely to cause harm to the Smithsonian. Any such Confidential Information, or copies or transcripts thereof, shall be returned to the Smithsonian upon completion of the work, or immediately destroyed upon request by the Smithsonian.

Contractor's Name:	
Purchase Order #:	
Individual's Name:	
Individual's Signature:	
Date:	

Background Investigations and Credentials for Contractors' Personnel

This information applies to the Contractor's employees and subcontractors, who provide services for the Smithsonian Institution (SI). All contractors are subject to SI security directives in effect during the duration of their contracts with the SI.

1. **Background Investigations.** Specifically, all Contractor's employees to be assigned to the SI under this contract shall be required to receive an SI Credential if their association with SI will be greater than thirty (30) days and they will need access to staff-only areas of SI controlled facilities and leased spaces. Prior to being issued this SI Credential, the Contractor's employees shall be required to undergo and pass an appropriate background investigation and complete security awareness training. The Contractor's employees whose associations with the SI shall be less than 30 days shall not receive a background investigation or SI Credential, however, they must be escorted by Credentialed personnel at all times when in staff-only areas of SI facilities. Upon successful completion of a background investigation, the Contractor's employees to be assigned to SI shall be issued an SI Credential that must be worn and visible at all times while on duty and within staff-only areas of SI facilities. If the nature of the work does not require escorted access to SI facilities, or when SI Credentialed staff can accompany contractors at all times, the Contractor and/or Contractor's employees may begin work prior to receiving an SI Credential. Contractor's and subcontractor's employees shall not be allowed unescorted access to SI staff-only areas until they undergo an adjudicated background check and receive an SI Credential.

2. **Forms, Information and Reviews Required.** The Contracting Officer's Technical Representative (COTR), or other designated SI employee, shall furnish the Contractor with an OF-306 (Declaration for Federal Employment form). An OF-306 must be completed by each person employed by the Contractor who shall be assigned to SI. Completed forms OF-306 must be returned by the Contractor to the COTR, or other designated SI employee, within ten (10) workdays from receipt of the forms. Upon notification from the COTR or designated SI employee the Contractor shall send each employee to be assigned to this contract to the SI Personnel Security and ID Office for fingerprinting. For contractors to SI organizations outside the Washington DC and New York City areas, SF-87 Fingerprint Cards shall be provided to the Contractor by the COTR or other designated SI employee. If necessary, the forms SF-87 shall be submitted by the Contractor with the OF-306. Based on the information furnished, the SI shall conduct a background investigation referred to as Special Agreement Checks (SAC). The SAC includes but is not limited to:

   - Security Agency Checks (record of previous suitability determinations)
   - FBI National Criminal History Check
   - Law Enforcement Checks

   SI shall review the investigation results and determine if the contractor and contractor's employees did not provide their true identities, or are otherwise not suitable for an SI Credential. SI shall provide the contractor with reasonable notice of the determination, including specific reason (s) the individual(s) has been determined to not have provided his/her true identity or is otherwise unsuitable for an SI Credential. The contractor or subcontractor has the right to answer the notice in writing and may provide documentation that refutes the validity, truthfulness, and/or completeness of the SI initial determination. After consideration of the initial determination and any documentation submitted by the contractor for reconsideration, the Director, Office of Protection Services (OPS), SI, or his/her designee, shall issue a written decision. The reconsideration decision by the Director, OPS, shall be final.

3. **Term Requirement for SI Credentials.** Throughout the life of the contract, the Contractor shall provide the same data for each new employee(s) or subcontractor(s) who will be assigned to this contract. The Contractor's SI Credentials shall expire annually and must be renewed, if necessary. It is the Contractor's responsibility to initiate the renewal process. The Contractor is not required to submit another set of background investigation forms for the Contractor's employees who have already been through this process.

4. **Relinquishing SI Credentials.** Upon expiration of the contract, or removal or termination of the Contractor's employees assigned to SI facilities, the Contractor shall return all SI Credentials issued to the Contractor's and /or subcontractor's employees to the COTR or other designated SI employee.

Background Investigations and Credentials for Contractors' Personnel

This information applies to the Contractor's employees and subcontractors, who provide services for the Smithsonian Institution (SI). All contractors are subject to SI security directives in effect during the duration of their contracts with the SI.

1. **Background Investigations.** Specifically, all Contractor's employees to be assigned to the SI under this contract shall be required to receive an SI Credential if their association with SI will be greater than thirty (30) days and they will need access to staff-only areas of SI controlled facilities and leased spaces. Prior to being issued this SI Credential, the Contractor's employees shall be required to undergo and pass an appropriate background investigation and complete security awareness training. The Contractor's employees whose associations with the SI shall be less than 30 days shall not receive a background investigation or SI Credential, however, they must be escorted by Credentialed personnel at all times when in staff-only areas of SI facilities. Upon successful completion of a background investigation, the Contractor's employees to be assigned to SI shall be issued an SI Credential that must be worn and visible at all times while on duty and within staff-only areas of SI facilities. If the nature of the work does not require escorted access to SI facilities, or when SI Credentialed staff can accompany contractors at all times, the Contractor and/or Contractor's employees may begin work prior to receiving an SI Credential. Contractor's and subcontractor's employees shall not be allowed unescorted access to SI staff-only areas until they undergo an adjudicated background check and receive an SI Credential.

2. **Forms, Information and Reviews Required.** The Contracting Officer's Technical Representative (COTR), or other designated SI employee, shall furnish the Contractor with an OF-306 (Declaration for Federal Employment form). An OF-306 must be completed by each person employed by the Contractor who shall be assigned to SI. Completed forms OF-306 must be returned by the Contractor to the COTR, or other designated SI employee, within ten (10) workdays from receipt of the forms. Upon notification from the COTR or designated SI employee the Contractor shall send each employee to be assigned to this contract to the SI Personnel Security and ID Office for fingerprinting. For contractors to SI organizations outside the Washington DC and New York City areas, SF-87 Fingerprint Cards shall be provided to the Contractor by the COTR or other designated SI employee. If necessary, the forms SF-87 shall be submitted by the Contractor with the OF-306. Based on the information furnished, the SI shall conduct a background investigation referred to as Special Agreement Checks (SAC). The SAC includes but is not limited to:

   - Security Agency Checks (record of previous suitability determinations)
   - FBI National Criminal History Check
   - Law Enforcement Checks

   SI shall review the investigation results and determine if the contractor and contractor's employees did not provide their true identities, or are otherwise not suitable for an SI Credential. SI shall provide the contractor with reasonable notice of the determination, including specific reason (s) the individual(s) has been determined to not have provided his/her true identity or is otherwise unsuitable for an SI Credential. The contractor or subcontractor has the right to answer the notice in writing and may provide documentation that refutes the validity, truthfulness, and/or completeness of the SI initial determination. After consideration of the initial determination and any documentation submitted by the contractor for reconsideration, the Director, Office of Protection Services (OPS), SI, or his/her designee, shall issue a written decision. The reconsideration decision by the Director, OPS, shall be final.

3. **Term Requirement for SI Credentials.** Throughout the life of the contract, the Contractor shall provide the same data for each new employee(s) or subcontractor(s) who will be assigned to this contract. The Contractor's SI Credentials shall expire annually and must be renewed, if necessary. It is the Contractor's responsibility to initiate the renewal process. The Contractor is not required to submit another set of background investigation forms for the Contractor's employees who have already been through this process.

4. **Relinquishing SI Credentials.** Upon expiration of the contract, or removal or termination of the Contractor's employees assigned to SI facilities, the Contractor shall return all SI Credentials issued to the Contractor's and /or subcontractor's employees to the COTR or other designated SI employee.

SMITHSONIAN INSTITUTION

CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (COTR) DELEGATION OF AUTHORITY CLAUSE

1) Lynda Schmitz Fuhrig , of the Smithsonian Institution, is hereby designated Contracting Officer's Technical Representative (COTR) and authorized to act for and on behalf of the contracting officer in the administration of this contract with respect to:

   a) Resolution of issues that may arise between the contractor and the Smithsonian Institution in connection with such matters as acceptability of workmanship and other technical requirements;
   b) Evaluation on an overall basis of the acceptability of workmanship and contractor compliance with technical requirements; and
   c) The acceptance of all work performed under the contract and approval of all invoices.

2) The contractor shall make available such records, reports and facilities as may be required by the above named individual to effectively and efficiently fulfill COTR duties and responsibilities.

3) This delegation of authority does not authorize the above named individual to modify any of the contract clauses, provisions, terms or conditions of this contract. All authorities not herein delegated are retained and shall be executed only by the contracting officer.

Smithsonian Institution

SMITHSONIAN DIRECTIVE 931,
September 14, 2020,

Date Last Declared Current: February 23, 2023

USE OF COMPUTERS, TELECOMMUNICATIONS DEVICES, AND NETWORKS

I. PURPOSE

The Smithsonian Institution's (SI) computers, telecommunications devices, and networks are to be used for Smithsonian-related work or work performed by approved partners and affiliated organizations. Users must understand the rules for using these resources appropriately, and their role in protecting these resources from unauthorized use.

II. BACKGROUND

Information Technology (IT) Security is a critical element of risk management for all organizations today. As evidenced by the ever-growing list of high-profile and increasingly sophisticated security breaches profiled in the media, organizations are at high risk of attack from criminal activity, "hactivism," espionage, insider threats, terrorism, and accidental self-imposed incidents, resulting in large financial losses, reputational damage, business disruption, and other serious consequences. Protecting the Smithsonian and the resources entrusted to it requires a concerted effort and relies on the cooperation of all Smithsonian personnel who must understand how they fit into and affect the Institution's overall IT security posture.

An important aspect of IT Security is ensuring that everyone at the Smithsonian understands not only the security policies that apply to them, but also their own role in maintaining IT Security, and the consequences of non-compliance. Smithsonian personnel must have an understanding of the security risks in their IT environment and what they can and are expected to do to help protect the Smithsonian's resources.

III. APPLICABILITY

This directive applies to all staff, contractors, volunteers, interns, visiting researchers, and other affiliated persons who use Smithsonian computers, telephones, mobile devices, software applications, storage drives, websites, data, printers/copiers, and networks, including all hardware connected to Smithsonian computers and networks. The directive does not apply to public use of external-facing websites or use of guest WiFi networks by visitors from the general public.

IV. DEFINITIONS

A. **Affiliated Persons** — For purposes of this directive, the term "Affiliated Persons" is defined as the following: (i) contractors who perform work similar to Smithsonian employees, such as employees of temporary help firms; (ii) volunteers, as defined in SD 208, *Standards of Conduct Regarding Smithsonian Volunteers*; (iii) interns and Fellows, as defined in SDs 701, *Smithsonian Institution Fellows*, and 709, *Smithsonian Institution Interns*; (iv) emeriti, as defined in SD 206, *Emeritus Designations*; (v) Smithsonian Early Enrichment Center (SEEC) employees; (vi) visiting researchers, including scientists, scholars, and students; (vii) research associates, as defined in SD 205, *Research Associates*; (viii) employees of federal, state, and local agencies, approved partners or affiliated organizations working with SI employees at SI facilities and property; and (ix) Regents and Advisory Board members.

B. **Computer** — Any programmable electronic device, including servers, desktop and laptop computers, tablets, smartphones, and network devices, that can be used to input, process, or store information.

C. **Encryption** — Scrambling of data so that only someone with an access key can read it.

D. **Hardware** — Physical parts of computers and related devices. Examples include hard drives, processors, memory, monitors, keyboards, mice, and other input devices. The term "hardware" may also be used to refer to the devices themselves, such as desktop computers, laptops, servers, phones, tablets, storage devices, printers, copiers, and scanners.

E. **Mobile Device** — Any portable computer, such as a laptop, smartphone, tablet, or other portable device that can store or process data.

F. **Network** — A set of computers connected for the purpose of sharing resources.

G. **Passphrase** — Sequence of words or other text used in place of a password.

IV. DEFINITIONS (continued)

H. **Personnel** — Everyone who participates in the operation of the Smithsonian and the performance of its mission, including staff, contractors, volunteers, interns, Fellows, and other affiliated persons.

I. **Phishing** — The practice of sending fraudulent emails in order to induce individuals to reveal information or click on malicious links/attachments.

J. **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.

K. **Sensitive Data** — Sensitive data includes personally identifiable information (PII), Payment Card Information (PCI), system access credentials, financial account information, security information, protected intellectual property, and other information whose access by the wrong people would be detrimental to the Smithsonian or its customers and stakeholders.

L. **Software** — The programs and instructions that run a computer, as opposed to the actual physical machinery and devices that make up the hardware. Examples include operating systems, internet browsers, browser extensions and plug-ins, business applications, productivity tools, software utilities, etc.

M. **Telecommunications Device** — Any electronic device used for communication over a network.

N. **User** — Anyone who accesses or makes use of Smithsonian computers, networks, and telecommunications devices.

V. POLICY

A. Rules for Users

Rule 1: Do Not Expect Privacy

The Smithsonian Institution’s computers, telecommunications devices, and networks are Smithsonian property and are to be used for Smithsonian-related work or work performed by

V. POLICY (continued)

approved partners and affiliates. This provision applies without regard to the location of the Smithsonian computer or telecommunications device.

Emails, documents, text messages, voice mail, or other files or data created, transmitted, or received while using Smithsonian computers, telecommunications devices, or networks are the property of the Smithsonian.

Users should have no expectation of privacy in email (including private password-protected email accounts), internet usage, text messaging, voice mail, video/teleconferencing, system access, usage logs, or other files or data created, transmitted, or received while using Smithsonian computers, telecommunications devices, or networks.

The Smithsonian has the right to monitor the use of its computers, telecommunications devices, and networks, and may monitor, access, inspect, store, or disclose any emails, documents, text messages, voice mail, or other files or data created, transmitted, or received while using Smithsonian computers, telecommunications devices, or networks.

In addition, Smithsonian records are subject to the Institution's records disclosure policy and may be publicly released in compliance with SD 807, *Requests for Smithsonian Institution Information*.

Incidental and occasional personal use is permitted, provided it does not interfere with the conduct of normal Institution business, does not cause expense or security risk to the Smithsonian, and meets the requirements of the other sections of this document. Such personal use does not create a user right of privacy, as any such personal use is subject to monitoring by the Smithsonian and the other provisions of Rule 1 described above.

Rule 2: Sign User Agreement

All users of Smithsonian computers, telecommunications devices, or networks must sign a user agreement (please see Appendix) before accessing a Smithsonian computer, telecommunications device, or network.

Rule 3: Complete Security Awareness Training

Personnel with an SI network account must complete the Smithsonian-approved online Computer Security Awareness Training (CSAT) annually, which includes reviewing and renewing acceptance of this directive. New users must complete this training within 30 days of SI account activation.

Personnel without an SI network account must complete Information Security Awareness Training (ISAT) annually.

V. POLICY (continued)

Personnel who perform IT management functions (such as development, administration, support, and security), as well as those people with elevated privileges on SI systems, may be required to complete additional role-based security training.

The Office of the Chief Information Officer (OCIO) periodically sends out computer security alerts, newsletters, and other awareness materials. Personnel are expected to review this information and apply it to their use of Smithsonian systems.

OCIO also periodically conducts phishing simulations to evaluate how susceptible personnel are to phishing and to determine the need for additional awareness training.

See IT-930-05*, Computer Security Training & Awareness*, for more information on security training and awareness requirements.

Rule 4: Provide Encryption Keys

Because data contained on Smithsonian computers, telecommunications devices, and networks are not private, users are required to provide their encryption keys on request to their supervisors, the Institution's director of IT Security, or the Office of the Inspector General (OIG).

Rule 5: Use Computers, Telecommunications Devices, and Networks Appropriately

Smithsonian users must not:

- harass or threaten other users or interfere with their access to Smithsonian computing or telecommunications facilities
- send, forward, or request racially, sexually, or ethnically offensive messages
- search for or use websites that involve hate groups or racially offensive or sexually explicit material
- seek, store, or transmit sexually explicit, violent, or racist images or texts
- send material that is slanderous or libelous or that involves defamation of character
- plagiarize
- send fraudulent email, texts, or other communications
- access computers, mailboxes, systems, or data for which they have not been authorized

V. POLICY (continued)

- intercept or otherwise monitor network communications without authorization

- misrepresent their real identity (*e.g.,* by changing the *From* line in an email). This does not include instances where an individual was granted permission to send email from another individual's account

- lobby an elected official

- promote a personal social, religious, or political cause, regardless of worthiness

- send or transfer malicious programs such as computer viruses, except for the forwarding of suspicious emails to the IT-Incident mailbox

- participate in gambling

- perform activities involving personal profit such as:

  — operating or promoting a personal business
  — performing paid work for another organization
  — online brokerage trading
  — selling personally owned items online, via email, or by phone
  — personal fund raising
  — performing any of the above-listed activities for a family member

- post personal opinions to a bulletin board, listserv, blog, social network, mailing list, or other external system using a Smithsonian user ID, except as part of official duties

- participate in activities that promote computer crime or misuse, including, but not limited to, posting or disclosing passwords, credit card and other account numbers, and system vulnerabilities

- violate any software licensing agreement or infringe upon any copyright or other intellectual property right

- disclose confidential or sensitive data without authorization

- create or maintain a personal website using Smithsonian computers, networks, and telecommunications devices

V. POLICY (continued)

- send mass mailings of a non-business nature
- send email announcements, other than those distributed by the Office of the Chief Information Officer (OCIO) or the Office of Public Affairs (OPA), to multiple groups that include most or all Smithsonian employees and affiliated persons. SD 112, *Internal Smithsonian Announcements*, provides guidance on Smithsonian-wide email announcements
- automatically forward Smithsonian email to a non-Smithsonian email account
- use any peer-to-peer file-sharing applications (such as BitTorrent)
- store Smithsonian sensitive data on personal devices, a personal cloud account, or a personal email account
- set up personal accounts on internet sites or services using Smithsonian account credentials, except where approved or instructed by OCIO
- use personal email accounts to conduct official Smithsonian business. If a personal email account is used, such as in emergency situations when Smithsonian accounts are not accessible or when a user is initially contacted through a personal account, the Smithsonian user must ensure that all Smithsonian records sent or received on personal email systems are forwarded to the person's official Smithsonian email account and captured and managed in accordance with Smithsonian recordkeeping practices.

Rule 6: Avoid Overloading System Resources

Each user should carefully evaluate his or her use of computers, telecommunications devices, and networks and:

- avoid sending large email attachments unless there is a business need
- delete email messages and files that are no longer needed in accordance with the official record retention guidance issued to his or her museum, research center, or office
- not overtax processing and storage capabilities or restrict access by others
- minimize downloading or streaming of audio and video files, including the use of online videogames, unless work-related.

V. POLICY (continued)

Rule 7: Comply with Software and Hardware Requirements

Users may not download, purchase, or install software unless it has been approved for use in the Technical Reference Model (TRM), IT-920-01, maintained by OCIO, and can operate on computer equipment specified in the TRM. SD 940, *Acquisition of Information Technology Products*, provides guidance on acquiring IT products. If users install unapproved software, it may have security vulnerabilities they are unaware of that will expose their computer and the SI network to attack.

Personnel may only purchase approved models of computers and devices. This ensures that the Smithsonian computing infrastructure remains stable, secure, and reliable.

Users may not add hardware to a computer, modify system files or security settings, or delete standard software on a computer without prior OCIO or unit IT support staff approval.

Personnel are not allowed to connect any network infrastructure devices (such as switches, routers, or wireless access points) to the SI network without approval from OCIO or their unit IT manager.

Only SI-owned devices or devices configured to SI standards by SI IT personnel may be connected to the **SI-Staff** network. Users should ask OCIO or their unit IT manager for the appropriate network to connect personal devices belonging to employees and affiliated persons, visitors, contractors, and others.

Copyrighted and licensed materials may not be used on a computer, other hardware, SInet, or the internet unless legally owned by the Smithsonian or otherwise in compliance with intellectual property laws. Users must read and understand all license material included with software. Personally owned software may not be installed on Smithsonian computers and devices.

Software must be retired or replaced when the version is no longer supported by the vendor/developer or when security updates are no longer being provided for that version, because it may be vulnerable to attack. When acquiring software for Smithsonian use, personnel must plan and budget for its periodic replacement.

OCIO may remove software from any SI computer if it presents a risk to the Smithsonian. Personnel must obtain approval from OCIO or their unit IT manager before reinstalling any removed software. OCIO may also block any computer containing risky software from the SI network.

Personnel must ensure that all computers (including mobile devices, laptops, and Windows-based tablets) that they purchase have full disk encryption enabled. Personnel must also ensure

V. POLICY (continued)

that the inventory management and theft deterrence software required by OCIO is installed on these devices.

All Smithsonian-owned computers, servers, and mobile devices must be configured in accordance with Smithsonian standards. Personnel must ensure that any new computers and devices that they acquire are configured to these standards or are submitted to IT support personnel for configuration of these standards.

All Smithsonian-owned devices are required to have up-to-date security patches. If a computer is found to be out of date on any security patches, it may be disabled until the patches have been installed. All employees are responsible for helping to ensure that their computer is kept up to date and secure by cooperating with, and following the instructions provided by, SI IT staff. Personnel must submit any new technologies, systems, cloud services, Web applications, websites, server applications, payment card processing solutions, or other IT services (or significant changes to existing ones) to the OCIO Technical Review Board for approval prior to acquisition or implementation. See SD 920, *IT Life Cycle Management*, for more information.

All purchases, especially those for IT systems and services, must contain appropriate security requirements such as SI-147B, *Smithsonian Institution Privacy and Security Clause*. Contact OCon&PPM if assistance is needed.

Rule 8: Protect Sensitive Data (including PII)

Users must take appropriate measures and exercise due diligence to protect sensitive data from loss, misuse, modification, and unauthorized access. Examples of sensitive data include Personally Identifiable Information (PII) (such as Social Security Numbers), payment card information (such as credit card numbers), proprietary information, and system security information (such as computer security deficiencies, User IDs [usernames], passwords, and network architecture information).

Everyone is responsible for protecting sensitive data and must apply appropriate safeguards. When handling sensitive data, users must:

- collect sensitive data only for a specific purpose and not retain it longer than required
- not transmit sensitive data over the intranet or internet unless encrypted. This includes all forms of transmission, including emails, file transfers, and Web forms. Users are responsible for obtaining the appropriate encryption tools and may contact OCIO for guidance in this area

V. POLICY (continued)

- only store sensitive data on a cloud service if it is an OCIO-approved service and the storage of any PII has been authorized by the Privacy Office. Users must also carefully manage who they give access to their cloud storage and the share links that they create

- not store sensitive data on non-SI-owned (e.g., personal) devices. This includes not synchronizing cloud storage files (such as those on Dropbox, OneDrive, and GoogleDrive) to personally owned computers and devices

- only store sensitive data on a laptop, phone, tablet, removable drive, or other mobile device if the device or data is encrypted

- not share sensitive data without approval of the appropriate management official

- mark or label media containing sensitive data to control and limit its distribution

- protect sensitive data that is in paper form by storing it in a secure location and shredding it when no longer needed

- follow procedures in SD 315, *Property Management Manual*, for properly disposing of surplus computers, smartphones, and other hardware to ensure that data are securely wiped from these devices before disposal

- conduct Smithsonian business via the official Smithsonian email system when using email.

Users must protect and handle PII in accordance with SD 118, *Privacy Policy*.

Users must protect any payment card data they handle in accordance with the requirements in SD 309, *Merchant Accounts, Payment Cards, and the PCI Data Security Standard*.

Rule 9: Apply Required Safeguards

To protect Smithsonian equipment and data, users are required to use safeguards that include:

- keeping laptops, tablets, cellular phones, and other mobile devices secure at all times, especially when traveling

- storing data that the user considers important where it will be subject to the Institution's automated backup process

V. POLICY (continued)

- accounting for hardware loaned for at-home use in a unit's personal property management records. Property custodians (PCs), or Accountable Property Officers (APOs) in the absence of a PC, are responsible for completing the required OCON 204, Personal Property Assignment/Personal Property Pass Form (available at the OCon&PPM Forms/Reference webpage), and obtaining the user's signature on the form at the time the property is assigned. Users are responsible for returning the assigned property when it is no longer required or the user's employment with the Smithsonian ends (see also SD 202, *Exit Clearances*). The PC, or APO, is responsible for taking necessary actions to ensure that the assigned property is returned when required and that the location of such property is accurately recorded in the unit's personal property management records

- using the Institution's centralized program for the disposal/surplus of old computers (managed by OCon&PPM), including sanitization of media containing SI data (see Section 8.4.2 of SD 315, *Property Management Manual* regarding the disposal of personal property).

- exercising appropriate precautions to protect computing devices and data when traveling. See OCIO document "Computer Security While Traveling"

- exercising appropriate precautions when using videoconferencing technologies. See OCIO page on videoconferencing.

All Smithsonian computers must have antivirus software provided by the Institution installed and active. The entire Institution's risk from the spread of malicious software is lowered when computers are properly configured to automatically update malware protection and to scan all files at the time they are received or used.

Any computers used to remotely access the Smithsonian network, including personally owned computers, must:

- have antivirus software installed. SI-provided antivirus licenses may be available for staff home use. See OCIO's Prism site for details; and

- use vendor-supported versions of operating system and internet browsers and keep them up to date with software patches (updates) from their vendors.

Personnel should leave SI computers turned on but logged off when they leave each day so that they can receive important updates and security scans.

V. POLICY (continued)

Users may not tamper with, disable, or intentionally bypass any IT security protections implemented by the Smithsonian.

Occasionally, high-risk situations may require user cooperation and urgent action to secure SI systems. For example, a staff computer may require extra scanning, IT staff may need to remotely access a computer/device, a computer may need to be taken off the network to remove malware, or users may be requested to install an urgent software update or reboot their computers. Personnel are required to cooperate with and help IT staff as best they can. Personnel must also pay attention to SI-wide emails providing security alerts and perform the requested actions to secure their devices.

Rule 10: Protect Access Credentials

Personnel are responsible for all actions performed using their access credentials and must take care to protect those credentials.

Personnel are required to exercise due diligence in protecting their logon credentials by:

- having a network password with at least 12 characters. It must not be found in a dictionary and not easily guessed. The use of passphrases is recommended;
- not keeping any passwords in writing unless locked in a secure location;
- using approved password management tools to assist in remembering and tracking passwords if needed (see Rule 7 regarding approved software);
- changing passwords every 180 days or more frequently, as appropriate;
- not re-using passwords;
- never disclosing or sharing passwords;
- not using the same password they use for Smithsonian systems on other (non-Smithsonian) systems. This includes externally hosted systems used for Smithsonian work (such as the Concur travel system);
- immediately notifying their supervisor and the OCIO Service Desk if they suspect their password has been compromised;
- immediately changing their password if it may have been compromised;

V. POLICY (continued)

- not sharing any accounts without receiving an approved waiver from OCIO;
- locking their desktop or computing device when leaving the immediate area;
- not displaying any cellular telephone, mobile device, or carrier wireless card passwords in public or attaching passwords to any devices; and
- never emailing passwords.

The sharing of accounts to log onto the network or SI computers/systems is not allowed without an approved security waiver, See IT-930-TN01 for information on security waivers.

Personnel must successfully complete a Smithsonian background check prior to receiving a Smithsonian network/computer account. See SD 224, *Identity Management Program,* and IT-960-TN12, *Active Directory Account and Password Requests*, for further details.

Rule 11: Report Security Incidents

All personnel are required to:

- promptly report any suspected security incidents, including the loss or theft of computers and devices, to the OCIO Service Desk in accordance with *IT-930-04, IT Security Incident Management*, and SD 119, *Privacy Breach Notification Policy*; and
- fully cooperate with security incident investigation and response activities.

Examples of security incidents that must be reported include, but are not limited to, the following:

- Loss or theft of computers and devices (in accordance with the guidance provided in Chapter 7 of the SD 315 *Personal Property Management Manual*);
- Potentially compromised access credentials or unauthorized access;
- Suspicious emails, phone calls, alerts, pop-up messages, or other unusual computer behavior;
- Inappropriate content on an SI system or website;
- Sensitive data accidentally or intentionally distributed to unauthorized persons or transmitted/stored without encryption;

V. POLICY (continued)

- Slow or unstable computer operations, such as when the cursor moves on its own, or files have been moved or tampered with;

- Violations of any of the requirements in this directive.

Rule 12: Use Cellular Phones and Mobile Devices Appropriately

Users are required to comply with the following when using a Smithsonian-issued cellular telephone, mobile device, or carrier wireless card:

- Read and comply with IT-980-TN01, *Smithsonian Cellular Telephone, Mobile Device, or Carrier Wireless Card Policy;*

- Follow all local, state, and federal telecommunications laws when using these devices;

- Understand that users may be required to reimburse the Smithsonian for any unauthorized cellular telephone, mobile device, or carrier wireless card service charges and/or those deemed to be personal use that exceeds permitted usages;

- Contact the OCIO Service Desk or the unit administrative officer to have cellular telephone/mobile device/wireless service discontinued and billing stopped when no longer required. Users are responsible for all billing charges associated with the device until they have done so;

- Understand that cellular telephones, mobile devices, and carrier wireless cards are not approved for transmitting sensitive data (including PII) and that users must exercise discretion when using them;

- Configure and periodically change a PIN code on the cellular phone to protect it from unauthorized use; and

- Only use Smithsonian-issued wireless cards in Smithsonian-issued computers, not personally owned computers.

B. Retention of User Agreements

Approved units or affiliated organizations that provide user accounts on Smithsonian networks must either store their own signed user agreements or provide scans of signed user agreements to OCIO. Copies of these agreements must be made available to OCIO upon request.

V. POLICY (continued)

C. Access to Files and Email

As described in Rule 1 above, personnel should have no expectation of privacy when using Smithsonian IT resources. Electronic files, email, and other data may be accessed by:

- Staff seeking to ensure efficient and proper operation of the workplace, particularly during unplanned employee absences. OCIO must first approve access, with concurrence from the IT support staff in the museum, research center, or office;

- Staff searching for suspected misconduct or malfeasance. The Office of Human Resources (OHR), the General Counsel, or the Office of the Inspector General (OIG) must first approve access;

- Staff representing the Smithsonian in litigation or a legal dispute, including responding to a discovery request, law-enforcement investigation, court order, or otherwise complying with a legal obligation;

- Staff responding to a public records request pursuant to SD 807, *Requests for Smithsonian Institution Information;*

- IT system administrators and their supervisors in the legitimate performance of their normal duties. They may not reveal information obtained in this manner unless authorized by OHR, except they may report any suspected criminal or policy violations to the employee's supervisor, senior management, the General Counsel or the OIG. Duties that allow a system administrator to access the files of other users include, but are not limited to:

  — maintenance or development
  — system security
  — correcting software problems
  — routine monitoring for compliance with this directive and for potential security incidents
  — security incident investigation and response; and

- Staff of the Smithsonian Institution Libraries and Archives (SLA) in the legitimate performance of their normal duties. Access must fall within its defined role as the Institutional Record Manager. The director in the museum, research center, or office must first approve access, with concurrence from the IT support staff for the museum, research center, or office. Duties that allow access include, but are not limited to:

V. POLICY (continued)

— identification of official and historical records
— development of unit-specific records management and retention guidance
— transfer of selected records to the Archives

D. Penalties

Penalties for violations of the user rules may include disciplinary action up to and including suspension without pay and termination of employment administered in accordance with Smithsonian personnel policies and procedures. Illegal activities will be reported to law-enforcement authorities for prosecution and punishment as provided by law.

VI. RESPONSIBILITIES

A. The **Chief Information Officer**:

- establishes computer security policies and standards; and
- grants waivers or exceptions to these policies and standards as appropriate.

B. The **Smithsonian Director of IT Security**:

- manages the computer security awareness program;
- administers the Institution's computer security awareness training;
- periodically distributes security awareness information via email notices and other mechanisms;
- leads the Smithsonian's security incident response activities; and
- monitors compliance with IT security policies.

C. The **Director, Office of Human Resources (OHR)**, ensures that:

- computer security awareness training is included in the orientation of new employees;

VI. RESPONSIBILITIES (continued)

- employees receive a copy of this directive and user agreement during orientation; and

- the Human Resource Management System (HRMS) includes employee training completion to ensure employee compliance.

D. The **director of each museum, research center, and office** ensures that:

- each SI network account user completes the online Computer Security Awareness Training (CSAT) annually;

- each person without an SI network account completes the Information Security Awareness Training (ISAT) annually;

- new users sign user agreements;

- signed user agreements are provided to OCIO;

- the importance of security awareness and complying with security policies is promoted to the unit's staff; and

- information about any suspected security incidents reported is passed on to the OCIO Security Operations Center (SOC).

E. **Users** ensure that they:

- read and understand the requirements in this directive before signing the user agreement;

- comply with the requirements in this directive; and

- report suspected violations of this directive to the OCIO Service Desk or their supervisor.

SUPERSEDES: SD 931, Use of Computers, Telecommunications Devices, and Networks, November 2, 2016.

INQUIRIES: Office of the Chief Information Officer (OCIO).

RETENTION: Indefinite. Subject to review for currency 36 months from date of issue.

SMITHSONIAN DIRECTIVE 931,
Appendix,
September 14, 2020,
Date Last Declared Current: February 23, 2023

USER AGREEMENT

I have read Smithsonian Directive 931, *Use of Computers, Telecommunications Devices, and Networks*, and understand that I am required to observe the policies and procedures stated in it. Furthermore, I understand that I am required to complete the online Computer Security Awareness Training (CSAT) within 30 days of the activation of my Smithsonian network account.

Print User's Name	**Unit**
User's Signature	**Date**

Please refer any questions to the Smithsonian Institution's Office of the Chief Information Officer (OCIO) Service Desk at 202-633-4000.