Smithsonian Institution

SMITHSONIAN DIRECTIVE 119,

September 12, 2018,

Date Last Declared Current: April 20, 2021

PRIVACY BREACH POLICY

1. PURPOSE

This Smithsonian Directive (SD) defines a breach of personally identifiable information (PII) and sensitive PII (sPII), outlines roles and responsibilities for reporting breaches of Smithsonian PII/sPII, and sets forth policies and procedures for determining how to mitigate the risk of harm to affected individuals when breaches occur. It is informed and supported by the Smithsonian Privacy Principles found in SD 118, *Privacy Policy*.

2. BACKGROUND

The Smithsonian Institution (SI) collects a broad range PII and sPII from Smithsonian employees, Affiliated Persons, and the public in order to fulfill its mission, and is committed to properly handling and protecting PII/sPII. Safeguarding PII at the Smithsonian and preventing its unauthorized acquisition, access, use, or disclosure are essential to ensure the Smithsonian retains the public trust. Although the SI is not subject to the federal privacy act or state breach reporting laws, through this policy, the SI incorporates current federal and industry standards and best practices regarding the breach of PII/sPII.

In 2010, the Smithsonian first promulgated SD 119, *Privacy Breach Notification Policy*, and established the Smithsonian Privacy Officer (SPO) position and the position of the Privacy Council Chair. In 2014, the Smithsonian issued SD 118, *Privacy Policy*, and the associated *Privacy Program Handbook*, which officially established the Smithsonian Privacy Program, the Smithsonian Privacy Principles, and policies and procedures for the collection, use, storage, and dissemination of PII/sPII.

3. APPLICABILITY

This directive applies to all Smithsonian employees and Affiliated Persons. For the purposes of this directive, the term Affiliated Persons is defined as: (i) contractors who access SI networks, facilities, or 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; (iv) emeriti, as defined in SD 206, *Emeritus Designations*; (v) visiting researchers, including scientists, scholars, and students; (vi) research associates, as defined in SD 205, *Research Associates*; and (vii) Regents and Advisory Board members.

This directive does not apply to collection objects, library and archival materials, their digital surrogates, or their supporting documentation (e.g., registrarial records) that contain PII/sPII. Those materials shall be collected, used, and protected in accordance with SD 600, *Collections Management*, and each unit's specific collection and archival policies. However, business or financial records (e.g., vendor enrollment forms) containing PII/sPII about individuals associated with a collection item (i.e., artists, donors, collectors, or researchers) is considered PII/sPII and, if breached, may be subject to this directive.

This directive addresses personal privacy interests only, and does not address other attributes of data that may warrant a higher level of care in its handling or disclosure. Several other Smithsonian Directives designate certain types of Smithsonian information or data as sensitive or confidential. (See Section 7, References.) As discussed in those directives, or as may be required by applicable law, information or data that falls within this designation may require a higher level of care in its handling and treatment.

4. POLICY

Smithsonian employees and Affiliated Persons shall exercise an appropriate degree of care when collecting, using, storing, or disseminating PII/sPII on behalf of the Smithsonian, to maintain its integrity, and prevent unauthorized access with the potential for misuse.

Breach Identification and Reporting

A breach is defined as a *suspected* or *confirmed* compromise, loss of control, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose.

The Smithsonian established the Smithsonian Privacy Council (Privacy Council) to help manage and coordinate the Smithsonian's response to a breach affecting members of the Smithsonian Community. The members of the Privacy Council are as follows:

- The Smithsonian Privacy Officer (SPO)

- Chief Operating Officer (COO) / Under Secretary for Administration (USA)
- The Chief Information Officer (CIO)
- The Assistant Secretary for Communications and External Affairs (ASCEA)
- The Director of the Office of Government Relations (OGR)
- The Director of the Office of Human Resources (OHR)
- The Director of the Office of Protection Services (OPS)
- The General Counsel
- The Smithsonian Risk Manager
- The Smithsonian Enterprises (SE) CIO *Ad hoc* member

The Privacy Officer serves as the Privacy Council Chair (Chair).

SI employees and Affiliated Persons shall report all breaches, security incidents, and information spillage immediately, but no later than one (1) hour after discovery, to the OCIO Help Desk and/or OPS as described in SD 119 Appendix, *Privacy Breach Reporting and Notification Process* (SD 119 Appendix or Appendix). If in doubt, individuals should err in favor of reporting. The Smithsonian does not retaliate against individuals for good-faith reporting regardless of whether the report is substantiated. OCIO and OPS shall immediately relay all breaches to the Chair who, as appropriate, will convene the Privacy Council. The Privacy Council shall assess the reports provided by the Chair and provide feedback in a timely manner. Members of the Privacy Council shall also notify the Chair of policy or procedural deficiencies they identify that could prevent or mitigate breaches.

Assessment and Response Activities — Significant Risk of Harm

If the Chair finds that a breach could lead to a significant risk of harm to one or more affected individuals, the Chair shall report that breach to the Privacy Council as soon as practicable, and then update the Privacy Council as material developments occur. The Chair shall direct the breach investigation and mitigation activities, in consideration of the Council's recommendations and risk of harm as discussed in SD 119 Appendix.

Once the breach has been mitigated, the Chair shall ensure that all key facts related to the breach and the response are documented. The Chair will determine if, when, and how to notify affected individuals and others of the breach, taking into account the considerations provided in the Appendix. Additionally, in an effort to further mitigate the harm caused by the breach, the Chair may recommend to the Privacy Council that the Smithsonian offer credit protection services (e.g., credit monitoring, identity protection or restoration services) to be funded by the responsible unit, as determined by the Privacy Council.

Following significant breaches (i.e. breaches that could lead to a significant risk of harm), the Chair shall also consider whether policy or procedural changes should occur to address the identified deficiencies, and then collaborate with the Privacy Council and appropriate key stakeholders to effect those changes.

Assessment and Response Activities — Non-Significant Risk of Harm

If the Chair determines that a breach is unlikely to lead to a significant risk of harm, the Chair shall direct the investigation and mitigation activities with consideration given to the risk of harm as discussed in SD 119 Appendix. The Chair will determine if, when, and how to notify affected individuals and others of the breach, taking into account the considerations provided in the Appendix. Once the breach has been mitigated, the Chair shall ensure that all key facts related to the breach and the response are documented.

Violations and Penalties

Persons who mishandle PII/sPII shall complete privacy training, as directed by the SPO. Further, conduct that violates this policy may be subject to appropriate disciplinary measures, up to and including removal or disassociation from the Smithsonian Institution.

5. DEFINITIONS

Affiliated Persons: For the purposes of this directive, the term Affiliated Persons is defined as: (i) contractors who access SI networks, facilities, or 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; (iv) emeriti, as defined in SD 206, *Emeritus Designations*; (v) visiting researchers, including scientists, scholars, and students; (vi) research associates, as defined in SD 205, *Research Associates*; and (vii) Regents and Advisory Board members.

Breach: The *suspected* or *confirmed* compromise, loss of control, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose.

Information Spillage: Occurs when sensitive information (to include, but not limited to, PII/sPII) is placed on an information system that is not authorized to maintain such information. This often occurs when information initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity.

Personally Identifiable Information (PII): Information about living individuals which may or may not be publically available, that can be used to distinguish or indicate an individual's identity, and any other information that is linked or linkable to a living individual, such as

medical, educational, financial, or employment information.[1] Examples of PII include, but are not limited to:

- General Personal Data: full name, maiden name, alias, full date of birth;
- Address Information: street address or email address;
- Personal Identification Number: Social Security Number, passport number, driver's license number, taxpayer identification number, financial account number, credit card number;
- Security Information: password, mother's maiden name; and
- Personal Characteristics: photograph or voice file that identifies an individual fingerprint, handwriting, biometric data such as retina scan, voice signature, facial geometry.

Security Incident (Information Technology [IT]): 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.[2]

Sensitive Personally Identifiable Information (sPII): A subset of PII that, if disclosed or used in combination with other data, could lead to harm to the individual (i.e., identity theft with the intention to do financial harm). sPII generally falls into the following categories:

Category 1: sPII is the first and last name or last name and first initial in combination with one or more of the following data elements:

- Social Security Number or personal Tax Identification Number;
- Driver's license or Government-issued identification number;
- Credit card number with or without an access code;
- Bank account number with or without a personal identification number or password; or
- Medical information (i.e., a diagnosis or condition).

Category 2: Physical sPII, such as biometric identifiers: iris scans, retina scans, fingerprints, voiceprints, are stand-alone data elements that are considered sensitive because of the possibility of increased risk to individuals if the information were to be compromised.

Smithsonian Units (Units): Collectively refers to all Smithsonian museums, research centers, and offices.

---

[1] Per Office of Management and Budget (OMB) M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, "[I]t is important to recognize that information that is not PII can become PII whenever additional information becomes available — in any medium or from any source — that would make it possible to identify an individual."

[2] An IT security incident can also be a breach if PII/sPII is involved.

6. RESPONSIBILITIES

Under Secretary for Administration (USA) oversees the Privacy Office. The USA is a member of the Privacy Council, and shall serve as the Privacy Council Chair or appoint a designee to serve on his/her behalf in the absence of the SPO.

Assistant Secretary for Communications and External Affairs (ASCEA) shall review and approve all external and Smithsonian-wide communications regarding breaches, except for those involving the Executive or Legislative branch of Government. The ASCEA, or his/her designee, shall lead, after consultation with the Chair, the response to all media inquiries pertaining to breaches. The ASCEA, or his/her designee, shall serve as a member of the Privacy Council.

The General Counsel shall provide legal advice, including on any Smithsonian legal or regulatory obligations, in the event of a breach. The General Counsel, or his/her designee, shall serve as a member of the Privacy Council.

The SPO shall serve as the Chair of the Smithsonian Privacy Council unless the SPO position is vacant, at which time the Under Secretary for Administration, or his/her designee, shall serve.

The Privacy Council Chair (Chair) shall take steps to ensure that all Smithsonian breaches are identified, tracked, mitigated, and documented in an effective, consistent, and timely manner consistent with this directive and associated Appendix. The Chair shall have the discretion to determine whether a breach, once identified, will lead to significant risk of harm which will then dictate notification to, and convening of, the Privacy Council. After consulting with the Privacy Council, the Chair shall determine when, who, and how to notify of a breach. The Chair shall also direct that, as part of remediation measures, the unit or individual(s) that caused the breach, receive privacy training. In addition, the Chair is responsible for keeping the Under Secretary for Administration, or his/her designee, abreast of all critical, sensitive, and controversial developments on breaches. The Chair shall review SD 119 and SD 119 Appendix at least annually to ensure it remains current and accurate, and coordinate updates when needed. The Chair shall also periodically, but not less than annually, convene the Privacy Council to hold a tabletop exercise and capture lessons learned to help ensure that members of the Council are familiar with this directive, the associated Appendix, and their roles and responsibilities in the event of a breach. The SPO shall serve as the Chair of the Smithsonian Privacy Council. In the absence of the SPO, the Under Secretary for Administration, or his/her designee, will serve as the Privacy Council Chair.

The CIO is responsible for monitoring the Institution's computer systems and networks (except for Smithsonian Enterprises' [SE] systems and networks). The CIO shall manage the SI Incident Response process, to include notifying the Chair when a security incident involves PII/sPII. The CIO shall ensure that all necessary IT technical support is provided in response to a breach, such as determining what information was affected and resolving any identified

security deficiencies that allowed the breach to occur. The CIO shall ensure that the requirements of Technical Note: IT-930-TN30, IT Security Incident Response Procedures and the *PCI Incident Response Plan* occur as applicable. The CIO reports breaches to the U.S. Computer Emergency Readiness Team (US-CERT), per IT-930-TN 30 requirements related to US-CERT reporting of IT security incidents. The CIO shall serve as a member of the Privacy Council.

The Smithsonian Enterprises (SE) CIO is responsible for monitoring SE applications, systems, and networks, and shall report any incidents involving PII/sPII to the Chair. The SE CIO shall ensure that all necessary IT technical support is provided in response to a breach, such as determining what information was affected and resolving any identified security deficiencies that allowed the breach to occur when SE's computer systems are involved in the breach. The SE CIO is an *ad hoc* member of the Privacy Council.

The Smithsonian Risk Manager shall provide the Privacy Council with information about any available insurance coverage relevant to a breach and for providing any required notice of a breach to insurance carriers. The Risk Manager shall serve as a member of the Privacy Council.

The Director of OPS is responsible for monitoring the Institution's physical security systems and for taking action to investigate and correct any physical security defects that may have permitted or been caused by a breach. OPS is responsible for promptly relaying any physical breach reports involving PII/sPII it receives to the Chair, and any IT-related breaches to the OCIO Help Desk. The Director of OPS shall serve as a member of the Privacy Council, and, in consultation with the Chair, shall coordinate with law enforcement agencies in responding to a breach of PII/sPII.

The Director of the Office of Government Relations (OGR) shall coordinate all communications and reports regarding breaches to the Executive or Legislative branch of Government as the Privacy Council finds appropriate. The Director of OGR shall be a member of the Privacy Council.

The Director of the Office of Human Resources (OHR) is responsible for providing policy guidance and assistance to Smithsonian Institution staff concerning employment and personnel matters. OHR maintains the Institution's official personnel records and works with units on procedures for how to handle employee and personnel information and documentation which routinely contain employee PII and sPII. OHR shall assist managers and supervisors in determining appropriate corrective measures and disciplinary actions when privacy breaches are substantiated. The Director of the OHR shall serve as a member of the Privacy Council.

Unit Directors shall ensure that all SI employees and Affiliated Persons within their unit comply with the requirements set forth in this directive, including participating, as necessary, in the Chair's investigation of a breach. Unit Directors shall also ensure that SI employees and Affiliated Persons complete privacy training, as part of breach remediation measures, as required by the Chair.

Unit Information Technology (IT) Directors will immediately notify OCIO when they detect or become aware of a breach to their unit's IT applications or systems.

The OCIO Help Desk is responsible for notifying the OCIO Director of IT Security, or the Security Operations Center (SOC), when they receive reports of possible security incidents, and for notifying the Smithsonian Privacy Officer whenever a privacy breach report is received.

Contracting Officers and the Contracting Officers' Technical Representatives (COTRs) shall take steps to ensure that the vendors they oversee are aware of the requirements of this directive, including the requirement to report breaches within a defined time frame and promptly respond to breach mitigation activities.

SI Employees and Affiliated Persons shall exercise an appropriate degree of care when collecting, using, storing, or disseminating PII/sPII, and shall cooperate, upon request, in the Chair's investigation of a breach. SI employees and Affiliated Persons shall also, as part of breach remediation measures, complete privacy training as required by the Chair.

7. REFERENCES

Smithsonian Documents:

SD 118, Privacy Policy and *Privacy Program Handbook*

SD 103, Smithsonian Institution Standards of Conduct

SD 309, Merchant Accounts, Payment Cards, and the PCI Data Security Standard

SD 606, Research Involving Human Subjects

SD 609, Digital Asset Access and Use

SI 147B, Smithsonian Institution Privacy and Security Clause and Usage Guide

Technical Note: IT-930-TN30, IT Security Incident Response Procedures

Federal Guidance:

Federal Information Security Modernization Act of 2014

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013

NIST SP 800-61, Computer Security Incident Handling Guide, August 2012

NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010

Office of Management and Budget (OMB) M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, January 2017

OMB Circular A-130, Managing Information as a Strategic Resource, July 2016

SUPERSEDES:	SD 119, June 24, 2010
INQUIRIES:	Smithsonian Privacy Office (SPO)
RETENTION:	Indefinite. Subject to review for currency 36 months from date of issue.
