



SNAAP PARTICIPATION AGREEMENT – 2022 SNAAP SURVEY

I. Purpose of SNAAP Survey

- a. The Strategic National Arts Alumni Project Participation Agreement (“Agreement”) is entered into between the Strategic National Arts Alumni Project (“SNAAP”) and [] (“Participating Institution”).
- b. The SNAAP survey is an online survey, data management, and institutional improvement system designed to enhance the impact of arts-school education. SNAAP provides national data on how artists develop, helps identify the factors needed to better connect arts training to artistic careers, and allows education institutions, researchers, and arts leaders to look at the systemic factors that help or hinder the career paths of arts-school alumni.

2. SNAAP Procedures and Safeguards

- a. SNAAP Survey administration protocol is approved by The University of Texas at Austin **Institutional Review Board (IRB)**.
- b. SNAAP uses public key encryption with an SSL connection to support the secure transmission of data across the Internet. Access by SNAAP staff to servers storing institutional data is controlled by user IDs and passwords.
- c. SNAAP contracts with Indiana University’s Center for Survey Research to administer the survey. The servers storing institutional data are managed by CSR. The CSR computing environment has robust security, the details of which are listed below:

*The computing environment at the CSR requires and maintains a high level of computer and data security per the **policies governing IU information technology resources and data**. The University Information Technology Services Policy Office (UIPO) at IU provides a baseline level of enforced security requirements including protocols to prevent unauthorized access to IU computers. The CSR computing staff uses industry standard best practices as our security procedures. Each CSR workstation is updated daily with virus protection software. CSR endpoints are scanned daily for needed security patches and hot-fixes. The centralized security server deploys all needed Microsoft security patches each night and machines are audited weekly to verify security patches are up to date.*

The CSR employs the Principle of Least Privilege when assigning access rights to staff. The systems administration staff has designed a number of processes for preventing intrusions or data loss on the CSR's servers. Remote access to the servers is tightly controlled by user IDs, passwords, and two-factor authentication through DUO. Physical access to servers is restricted per the security protocols of **IU's data center**. Access to directories on the file servers is restricted to only those employees who need access. Security processes similar to those run on the workstations are used to prevent, detect, and repair security problems on the servers. The servers are located on a range of private IP addresses restricting their access from the outside world. The servers sit behind a network firewall, and employ their own machine firewall. IU provides security scanning of our servers to look for possible problems and the computing staff carefully monitors server event logs for possible attempts at intrusion.

Individual workstations are part of a Virtual Lan (VLAN) which allows even greater restriction of access. Any remote access requires remote authorization and a connection using an SSL VPN behind two-factor authentication.

The files on the servers are backed up each night, and all project data is encrypted at-rest within the backup. The file and web servers are virtual systems employing RAID 5 technology to ensure that a disk failure will not cause any loss of data. They are located in a modern class 4 data center designed to meet FEMA standards for surviving an F5 tornado among other natural disasters. The building is staffed 24x7 and employs all modern physical security measures.

The CSR uses 2048-bit public key encryption with a 128-bit SSL connection to ensure the security of survey and other sensitive data that are transmitted across the Internet. The digital certificates were issued by InCommon/COMODO and are used by the survey respondent's browser to verify that the user is connected to the website that matches the name in the URL. The browser and the server then encrypt and exchange keys that are used to encrypt the remainder of the session. Through the use of these keys, the data are transmitted using the SSL. The security procedures used by the CSR are equal to or surpass the requirements for transmitting confidential information.

- d. Institutionally identifiable SNAAP results shall not be made public by SNAAP except by mutual agreement between SNAAP and Participating Institution, or in accordance with any applicable law, such as the Texas Access to Public Records Act.
- e. SNAAP will partner with PCI (formerly Harris Connect) or a similar alumni tracking company to provide new and updated contact information for Participating Institutions alumni. Any new and updated contact information will be provided to Participating Institution following the administration of the survey. Participating Institutions can opt out of this free service; if the institution chooses not to utilize this service, the institution must notify SNAAP directly at a date to be determined.
- f. SNAAP project staff may use survey data in the aggregate for national reporting purposes. SNAAP may also make de-identified data available to outside researchers.

- g.** Participating Institution will be charged based on the number of arts degrees conferred by Participating Institution in 2019/20 (verifiable by IPEDS data), as reported to the U.S. Department of Education.

h. Participating Institution Procedures and Requirements

- i.** Participating Institution agrees to provide an alumni population data file containing contact information as defined by SNAAP population file guidelines. SNAAP will not use population file data for any purpose other than the SNAAP survey. SNAAP will not release contact information to a third party unless Participating Institution gives the express authority to do so (as in the case of PCI or other alumni search firm) or unless required to do so by law.
 - j.** Participating Institution will customize its survey administration on the secure online SNAAP interface. The Participating Institution's response rates, Institutional Reports and complete dataset (when available), and other information will be housed on the secure SNAAP interface and accessible to all Participating Institution authorized contacts.
 - k.** Participating Institution is encouraged to send general promotional announcements to its alumni about the survey, but will be asked not to contact individual alumni directly to recruit them for the project without prior approval from The University of Texas at Austin IRB. Participating Institution must present the SNAAP Survey as a voluntary activity; no coercion can be used to increase participation.
 - l.** Participating Institution must seek SNAAP's approval of any alumni participation incentives (e.g., lottery drawings and prizes) to ensure compliance with IRB requirements.
 - m.** Participating Institution shall pay SNAAP all applicable fees related to the survey within thirty (30) days of receipt of the survey invoice, unless alternate payment arrangements are requested.
- i. Use of Alumni Data**
- o.** Participating institutions will provide SNAAP with the following data elements (subject to change): first and last name, gender, mailing address, phone number, email address, degree pursued, major, level of degree pursued, cohort or graduation year, department/school/college information, and other information chosen by Participating Institution.
 - p.** With respect to its use and handling of personally identifiable data received from the Participating Institution, SNAAP will:
 - i.** Ensure the quantitative alumni survey responses provided to Participating Institutions are stripped of all identifiers so that alumni responses are anonymous to institutions. Note: open-ended alumni responses may contain identifiers.
 - ii.** Use such data only for the purposes of conducting studies designed to

improve arts training, inform cultural policy, and/or support artists as well as studies that evaluate the effectiveness of SNAAP survey methods in order to improve future data collection. SNAAP may make de-identified data available to interested and qualified researchers.

- iii. Only use alumni contact data for the purposes of inviting alumni to participate in the SNAAP survey, or to evaluate the effectiveness of survey administration methods;
 - iv. Use Secure Sockets Layer (SSL) software to encrypt information during transfer from Participating Institution to SNAAP;
 - v. Limit access to such data to representatives of SNAAP who have legitimate interests in the information for the purposes described above;
 - vi. Not provide Participating Institution's data to a third party except as permitted in this Agreement;
 - vii. Use the data in the aggregate for national and sector reporting purposes;
- q. Unless a Participating Institution opts out prior to providing its data files to SNAAP, SNAAP may partner with PCI or a similar alumni tracking company to update and correct alumni contact information provided by the Participating Institution. SNAAP will provide Participating Institution with the updated and corrected alumni contact information following the administration of the SNAAP survey to Participating Institution's alumni.
 - r. SNAAP may retain Participating Institution data in its database. The parties understand and agree that SNAAP will maintain survey response data for an indefinite period of time, in order to enable longitudinal study of arts career trends and other analyses.
 - s. The use of student data is regulated by the U.S. Family Educational Rights and Privacy Act ("FERPA"), which covers how educational institutions may share student data with outside organizations conducting research and assessment for the purpose of improving instruction.
- 3. Assignment.** This Agreement shall not be assignable by either party without the prior written consent of the other party.
- 4. Force Majeure.** Neither party shall be responsible or liable to the other party for nonperformance or delay in performance of any terms or conditions of this Agreement due to acts of God, acts of governments, wars, riots, fire, flood, or other causes beyond the reasonable control of the nonperforming or delayed party.
- 5. Limitation on Liability.** Participating Institution agrees that SNAAP, The University of Texas at Austin, and its trustees, affiliates, employees, agents, and contractors, shall not be liable to Participating Institution for any claims, liabilities, consequential or incidental damages, costs, or expenses relating to this Agreement for an aggregate amount exceeding the fees paid by Participating Institution to SNAAP.
- 6. Entire Agreement.** This Agreement constitutes the entire agreement between the parties regarding the subject matter described herein and supersedes any prior negotiations and

agreements. This Agreement may not be modified or amended in any respect except by a written agreement executed by both parties. The terms and conditions of this Agreement shall extend to, be binding upon, and inure to the benefit of the heirs, administrators, representatives, executors, successors and assigns of the parties.

IN WITNESS THEREOF, the parties hereto have executed this Agreement as of the Effective Date.

By: _____

By: _____

Date: _____

Date: _____

Lee Ann Scotto Adams
Executive Director, SNAAP

[Name]
[Title]