Taiko Community Alliance

Data Use Policy

TAIKO COMMUNITY ALLIANCE

Last updated 8.8.20231

1. Security Level Descriptions and Access

TCA's data systems are described in the document below. As an organization with stakeholders spread geographically, we manage approximately 30 different online-based software systems to enable the day-to-day business of our organization. These systems are categorized as Level 1, 2, or 3 to reflect the sensitivity of the information stored in each location, where a Level 1 designation indicates the most sensitive data and, consequently, the most highly-protected data.

a. Level 1

Personally Identifiable Information (PII) that requires the highest level of security and limited access. This also includes any information deemed by the TCA board as private or classified. Examples include but are not limited to:

i. Social Security Numbers
ii. Credit Card and payment information
iii. HR information:
    1. Payroll and personal financial information
    2. W9s and other tax information
iv. Un-approved meeting minutes
v. Financial reports
vi. Organizational finance information
vii. Completed Contracts and Agreements
viii. A list of systems that contain Level 1 information is available by request from the Executive Committee.

Approval Policy for access to Level 1 Data

Individuals with Level 1 access must be approved by the TCA Executive Committee. The Executive Committee must notify the Google Administrator when an individual is approved for Level 1 access.

b. Level 2

Personal contact information, TCA brand and messaging services. Examples include but are not limited to:

i. Phone numbers
ii. Email addresses
iii. Mailing addresses
iv. Administrative systems access:
    1. Website, social media, non-public program information (contracts & agreements, confidential program information)
    2. TCA meeting resources (Google Meets, Zoom login)

Approval Policy for access to Level 2 Data

Committee chairs may approve Level 2 security access, and must notify the Google Administrator of these changes.

c. Level 3

Public Information: Information that is accessible to the general public. No approval is necessary to access Level 3 data. Examples include but are not limited to:

i. Program publicity information
ii. Approved meeting notes
iii. Website information

2. Information Retention and Deletion Policy

a. Retention Policy

For the types of documents indicated below, TCA agrees to securely store records for the indicated amount of time. Hardcopy documents to be stored with financial documents maintained by TCA Treasurer.

i.

TYPE OF DOCUMENT	MINIMUM TERM
Program attendee registration info and agreements	5 years
Board applications and agreements	6 years
Personnel File Records (Medical records should be stored separately)	4 years (after termination)
I-9 forms (stored separately from regular personnel files)	3 years (after the date of hire or 1 year after termination)
W 9 Forms	1 year
W4 Forms	4 years
Equal Pay	2 years
Title VII Records	1 year
Payroll and Tax Records (Name, Address, SSN, wage rates, Hours worked, weekly	4 years

deductions, allowances, etc)	
Call Logs	7 years
Meeting Minutes (soft copy)	7 years
Financial Records (soft copy is ok)	7 years

b. Deletion Process

i. Hard Copy Documentation:
   1. When ready for deletion, all hard copy documentation will be securely destroyed (suggested methods below):
      a. Shredded
      b. Burned
      c. PII redacted and thrown away

ii. Soft Copy Documents and attachments will be electronically destroyed

iii. Email:
   1. Non-essential email should be deleted annually
      a. Essential email is defined as any messages or attachments necessary for archival use or future planning.
      b. Non-essential email is defined as any messages not deemed necessary for archival record keeping or future planning purposes.

3. Onboarding and Offboarding Process

When new volunteers or staff enter or depart the organization, the following protocol should be followed.

a. Email Address Use and Granting

i. TCA business must be conducted on an official TCA email address with @taikocommunityalliance.org domain. Volunteers and board members are expected to regularly check their @taikocommunityalliance.org email addresses as a primary form of internal communication. @taikocommunityalliance.org email addresses may not be forwarded to personal emails.

ii. Requesting an Email
   1. Request should be submitted via email to the Google Administrator with:
      a. First and Last Name
      b. Contact Phone Number
      c. Completed TCA Data Use Agreement

d. Any email lists to be updated
e. Level of security access and approval (Level 2 and 1 only)

2. Request Protocol
    a. Volunteer: Committee Chair submits the request
    b. Board Member: Board Secretary submits the request
    c. Staff: Supervising Board Member submits the request
3. Google Administrator will
    a. Confirm agreement to the TCA Data Use Agreement.
    b. Create an @taikocommunityalliance.org email address for the individual
    c. Add the new user to appropriate google list(s)

b. Email Lists (Google Groups)

i. Google Administrator will maintain a current list of Google Groups and members of each group. That list will be available to TCA Board Members and Committee Chairs.

ii. Google Administrator will send Committee Chairs a copy of their list annually. Committee Chairs are expected to respond to Google Administrator to verify accuracy of the list.

iii. Committee Chairs are responsible at all times for notifying the Google Administrator of:
    1. Change in membership
        a. If necessary, committee chair may approve Level 2 security access
        b. If necessary, committee chair must have Level 1 security access approved by the TCA Executive Committee
    2. Inaccuracies

iv. Committee Chairs will work with the Google Administrator to:
    1. Create group alias
    2. Forwarding and manage committee email
    3. Request new aliases
    4. Delete or remove distribution lists

v. Sunset and Renewal Process: Google Administrator will evaluate and update lists every two years.

c. Document and Information Sharing Policy

i. **Security Level.** Documents and information will be shared only within the TCA environment. Sharing is only allowed within populations of similar security level access.
   1. Level 1 information may only be shared with Level 1-approved individuals
   2. Level 2 information may only be shared with Level 2 or Level 1-approved individuals
   3. Level 3 information may be shared with anyone.

ii. **Meeting Notes.** Meeting notes and committee documents should be shared with an email distribution list instead of individuals whenever possible.

d. Personnel Change Process

i. Committee chairs are responsible for notifying the Google Administrator of any changes in committee membership within 7 days of personnel change via email and should share the following information:
   1. Name of individual(s) involved.
   2. Reason for change.
   3. Email list(s) affected by the change.
   4. Google documents affected by the change.
   5. Change of ownership for documents.

ii. Within 48 hours, the Google Administrator will make the following adjustments and confirm the completed changes via email.
   1. If an individual will no longer be a TCA Committee Member
      a. Suspend the G-Suite account of the user.
      b. Change password(s) to all Level 1 and Level 2 TCA assets individuals had access to.
   2. If the individual is changing Committees.
      a. Update email list(s) affected by the change.
      b. Make appropriate adjustments to Google document ownership.

4. Systems Access

a. Requests for access to TCA Systems should be directed to the Executive Committee. See Section 1 for Data Access Approval Policy.

5. Password Best Practices

a. Passwords should be changed every 90 days [alternatively, implement two-step authentication]
b. Passwords should contain more than 7 characters, one capital letter, one number, and one special character.

6. TCA Information Security Requirements

a. TCA Information Security Requirements below, in Addendum A, For TCA partner(s) For third party external users, e.g., Discover Nikkei, or folks wanting access to Census information.

Addendum A

TCA Information Security Requirements For TCA Partner(s)

Last updated May 9, 2023

INFORMATION SECURITY REQUIREMENTS

1. TCA Partner shall maintain the privacy of personal information and confidential data as confidential information. TCA Partner shall not use, disclose, or release confidential information contained in TCA records without permission from the TCA Board of Directors.

2. TCA Partner shall maintain the privacy of confidential information and shall be financially responsible for any notifications to affected persons (after prompt consultation with the TCA) whose personal information was disclosed by any security breach relating to confidential information resulting from TCA Partner's or its personnel's acts or omissions.

3. TCA Partner is required to maintain adequate security sufficient to protect sensitive TCA data to which they have access.

4. TCA Partner shall require all its affiliates and subcontractors, as a condition to their engagement, to protect all sensitive TCA data.

5. TCA Partner shall not use or disclose TCA Protected Data other than to carry out the purposes of this agreement.

6. TCA Partner shall not disclose any TCA Protected Data other than on a "need to know" basis.

7. TCA Partner shall develop, implement, maintain and use appropriate administrative, technical and physical security measures, which may include but not be limited to encryption techniques, to preserve the confidentiality, integrity and availability of all such TCA Protected Data.

8. Upon the termination or expiration of this Agreement, or at any time upon the request of the TCA, TCA Partner and its subcontractors shall return all TCA Protected Data (and all copies and derivative works thereof made by or for TCA Partner). Further, TCA Partner and its subcontractors shall delete or erase such TCA Protected Data, including copies and derivative works thereof, from their computer systems.

9. TCA Partner shall report, in writing, to the TCA any use or disclosure of TCA Protected Data not authorized by this Agreement or authorized in writing by the TCA, including any reasonable belief that an unauthorized individual has accessed TCA Protected Data. This report shall be made to the TCA's primary contact and TCA's Board of Director. It shall include details relating to any known or suspected security breach of TCA Partner's system or facilities which contain TCA Protected Data or any other breach of Protected Data relating to this Agreement. This report shall be made within two (2) days after discovery, if the information was, or is reasonably believed to have been, acquired by an unauthorized person.