Trusted CI Collaborator Information Policy

Effective Date: May 13, 2020, V4
Distribution: Public
Authority: Von Welch

---

1 Procedures

Trusted CI seeks to balance two principles:

1. Trusted CI controls the management and distribution of confidential data such that community members are comfortable sharing such data with Trusted CI during the course of collaborations, engagements, etc.
2. Trusted CI seeks to share information broadly with the community to facilitate learning from common experiences.

To that end, this policy defines how Trusted CI distinguishes and manages confidential data from data it can broadly disseminate.

1.1 Handling Collaborator Information

Trusted CI will apply the following practices to handling collaborator information unless otherwise agreed (for example, in an Engagement Plan):

1. All Engagement Plans (or other planning documents) should explicitly call out what resulting products will be public. The goal is to make as many products public as possible to foster broad impact from the engagement.
2. Any data, documents, communications, etc. that a collaborator with Trusted CI wishes to remain confidential shall be marked or otherwise clearly indicated as "confidential" by the collaborator.

3. Trusted CI staff handling confidential data should ensure it is labeled by the Trusted CI Data Labeling Policy as either 'Internal Use Only', 'Release to <appropriate party>' or 'Release to <appropriate party> after <date>' as appropriate.
4. Trusted CI team members must ensure they do not share confidential information outside of Trusted CI.
5. Trusted CI team members may not use confidential data for research and other purposes not related to Trusted CI without explicit permission of the relevant project.

1.2 Exceptions to this policy

Trusted CI is committed to confidentiality with collaborators, however they should be aware of the limits of what Trusted CI can guarantee.

1. Trusted CI is a virtual organization comprising a number of institutions. Trusted CI will share information when required by law as determined by one of their institutional general counsel's offices.
2. Collaborator information will be shared within the Trusted CI project for internal business purposes such as quality control, reporting, and conflict-of-interest management.
3. The fact that Trusted CI is collaborating with a project and a high-level description of that collaboration will be reported to the National Science Foundation and publicly disseminated.

When Trusted CI is required to share collaborator information outside of Trusted CI, it will do its best to minimize that sharing and inform the relevant parties.

2 Scope: Defining "Collaborator Information"

Collaborator information is any information received from a member of Trusted CI's community, or information derived from such information. Examples include:

1. Information received during an engagement. For example, during discovery or during conversations.
2. Reports and other products created by Trusted CI during an engagement.
3. Communications with Trusted CI about cybersecurity generally that reveal operational cybersecurity details about the communicating party.
4. Information received by Trusted CI about proposals being written by community members, often in the form of queries in regards to Trusted CI's participation.
5. Non-public source code and any undisclosed (to the public) weaknesses discovered by Trusted CI in software.

Trusted CI does not normally accept or handle data falling under a regulation such as HIPAA or NIST 800-171, and hence such data is out of scope of this policy.

3 Policy Description

In the course of its activities, particularly, but not only, Engagements, Trusted CI will obtain or develop information about other projects which those projects consider sensitive and confidential between Trusted CI and themselves. This policy defines “Collaborator Information” and documents Trusted CI’s principles in handling such information.

4 Reasons for this Policy

This policy exists to ensure uniform handling of collaborator information across the Trusted CI project and to provide assurances and details to Trusted CI collaborators on how Trusted CI will handle their information.

5 Change Log

Date	**Description of Change**	**Version Number**
2/7/2020	Initial version	V1
3/10/2020	Renamed to “Collaborator Information Policy”	V2
3/20/2020	Modified to use new Trusted CI Policy Template. Added Section 4, otherwise just shuffled text.	V3
5/13/2020	Modified to final to address leads feedback	V4