Trusted CI Staff Onboarding / Offboarding Procedures

Effective Date: February 4, 2021
Distribution: Public
Authority: Trusted CI Information Security Office
Last reviewed by the ISO on May 20, 2021

---

1 Procedures

This section describes the process for handling the onboarding or offboarding of Trusted CI personnel.

1.1 Role Assignments

This section lists specific roles that have key responsibilities in either the onboarding or offboarding process. The current Trusted CI personnel (or in some cases, IU staff) are listed for roles when applicable; these may need to be redacted prior to publication of this document.

- New Staff Member (NSM) - the Trusted CI personnel to be onboarded
- Exiting Staff Member (ESM) - the ex-Trusted CI personnel to be offboarded
- Supervisor (SUPV) - Not a role per se, but the requestor for either the onboarding or offboarding request; note, person must be the supervisor or Trusted CI liaison with the authority to request the onboarding/offboarding of either NSM or ESM
- Project Manager (PM) - person acting as 'project manager' for Trusted CI
    - Redacted-For-Privacy
- IT Support (ITS) - person providing IT support for Trusted CI; most likely an IU employee

    - Redacted-For-Privacy
- Information Security Office (ISO) - people responsible for tracking onboarding/offboarding process; updating information security documents (e.g., ASAPS); informing NSM and-or SUPV when necessary; and setting permissions on assets out of scope of ITS or PM

1.2 Onboarding New Personnel

Steps describing the process to follow for onboarding a NSM. The sophistication of this process described below is (i) to capture some complexities with being a multi-institution organization, (ii) be detailed sufficiently enough to handle turnover in key roles, and (iii) to lay the burden of task management on the ISO. That is, other than the SUPV having knowledge to initiate the process, the ISO informs all participating roles of what their duties are at each phase, while tracking the process.

- SUPV Task-1: Gather the necessary information about NSM, including:
    1. **NSM's email address**; note, the email address used must fall under the authoritative domain of the SUPV, i.e., the SUPV is NSM's supervisor in G Suite at their home institution[1]
        - If 1. Above is not possible, then SUPV must request of ITS an IU Affiliated account for NSM; the IU Affiliated email address is the one used
    2. **NSM's adopted asset management roles**, if any, e.g., NSM will be owner of Trusted CI's YouTube account
    3. **NSM's effort level** in Trusted CI
    4. **NSM's additional mailing lists**; see ISO Task-3 below for "if necessary" options
    5. **NSM's institutional staff page URL**
- SUPV Task-2: Submit request to onboard NSM to 'security@trustedci.org', including all items gathered in Task-1
- ISO Task-1: Register request in ticket system
- ISO Task-2: Through ticket system, acknowledge SUPV's request
- ISO Task-3: Through ticket system, request ITS to add NSM to the following email lists:
    1. ctsc-team-l@list.iu.edu [List interface]
    2. ctsc-discuss-l@list.indiana.edu
    3. ctsc-announce-l@list.iu.edu

    Add to the following as necessary:
    4. Redacted-For-Privacy
- ISO Task-4: Through ticket system, request PM to:
    1. verify that NSM has enabled Google's 2-Step Verification or equivalent; note, In most circumstances this is a self-reporting task on the part of the NSM as some

[1] This policy is necessary because it is extraordinarily difficult to change ownership in G Suite after an employee leaves without a supervisory role on Google Drive.

institutions enforce their own two factor implementations on their staff and this would not require this check (ie. Indiana, Illinois, UWisc).
    2. enable access to the Google Drive folder 'Trusted CI [INTERNAL]' by *sharing* NSM's email address
    3. send NSM a link to the active policy documents folder; inform NSM that they must familiarize themselves with all active policies found there; and that NSM must notify PM when task is complete
- ITS Task-1: respond to the ticket-system generated email for ISO Task-3 when complete
- PM Task-1: respond to the ticket-system generated email for ISO Task-4 when complete
- ISO Task-5 (BARRIER: ITS Task-1, PM Task-1): Through ticket system, request SUPV 'introduce' NSM to staff (i.e., send introduction to Redacted-For-Privacy)
    - ISO ensures that SUPV sent introduction to staff
    - Note, as an optional task, specific and-or institutional meeting owners can add NSM to their meeting calendars, and other institution specific tasks, but this is not tracked by ISO
- ISO Task-6: Through ticket system, request PM to:
    1. update agenda in order to introduce NSM on next All Hands Call
    2. add NSM to calendar invite for All Hands Call
    3. add NSM to Slack channel
    4. add NSM to the Trusted CI effort reporting spreadsheet
    5. add NSM to "Who we are" page on trustedci.org website
- ISO Task-7: Through ticket system, request ITS to:
    1. grant NSM author access to Trusted CI blogger.com account
    2. grant NSM author access to Trusted CI SquareSpace account
- PM Task-2: respond to the ticket-system generated email for ISO Task-6 requests when complete
- ITS Task-2: respond to the ticket-system generated email for ISO Task-7 requests when complete
- ISO Task-8 (BARRIER: PM Task-2, ITS Task-2, ISO Task-5): Inform Leadership onboarding for NSM has completed

1.3 Offboarding Exiting Staff

Steps describing the process to follow for offboarding a ESM. As with 'onboarding', the process appears complex, but that is mostly in order to allow the ISO to track progress.

- SUPV Task-1: Submit request to offboard ESM to 'security@trustedci.org'
    - Note, if ESM does not have a SUPV, then the PM acts as the SUPV for purposes of these offboarding procedures
- ISO Task-1: Register request in ticket system
- ISO Task-2: Through ticket system, acknowledge SUPV's request
- ISO Task-3: Through ticket system, request PM to have ESM transfer ownership of Trusted CI documents under 'Trusted CI [INTERNAL]' to a current personnel

    - Note, if ESM is unable to transfer ownership, PM should contact SUPV (i.e., ESM's G Suite supervisor) to transfer ownership to a current personnel
- ISO Task-4: Identify all *special access* ESM had via ASAPS documents; remove said permissions; and change shared secrets if any
    - Note, if ESM was owner in any ASAPS, assign SUPV as owner of ASAPS, informing SUPV of new responsibility
- ISO Task-5: Through ticket system, request ITS to remove ESM from:
    1. Trusted CI blogger.com account
    2. Trusted CI SquareSpace account
    3. ctsc-team-l@list.iu.edu [List interface]
    4. ctsc-discuss-l@list.indiana.edu
    5. ctsc-announce-l@list.iu.edu

    Remove from the following as necessary:
    6. remove access to Discord chatroom
    7. Redacted-For-Privacy
- ITS Task-1: respond to the ticket-system generated email for ISO Task-4 requests when complete
- PM Task-1: respond to the ticket-system generated email for ISO Task-5 request when complete
- ISO Task-6 (BARRIER: PM Task-1): Through ticket system, request PM to:
    1. remove ESM's 'sharing' permission from 'Trusted CI [Internal]'
    2. run CloudPerm 'revoke-access.sh' script
    3. remove ESM from calendar invite for All Hands Call
    4. remove ESM from Slack channel
    5. remove ESM from the Trusted CI effort reporting spreadsheet
    6. remove ESM from "Who we are" page on trustedci.org website or add them to the Alumni section.
    7. update agenda in order to inform current staff on next All Hands Call of ESM's departure
        - note, this will allow institutional meeting owners to remove ESM from calendar invites
- PM Task-2: respond to the ticket-system generated email for ISO Task-6 requests when complete
- ISO Task-7: If ESM had access to the Trusted CI Youtube account, submit 'infrastructure change request' change the Youtube account 'shared' password by submitting an infrastructure change request in order to have the Youtube Account Manager change the password and distribute new secret to remaining personnel with authorized access[2]

[2] When we switch to a Brand Account for YouTube access, this procedure will change to only needing to remove ESM's Google ID from the Brand Account (similar to removing them from Blogger): https://docs.google.com/document/d/1qGLSKnkYjDfT-i9NzUaQkTY5N112y8aWsKnGjj6WDS0/edit?usp=sharing

- ISO Task-8 (BARRIER: PM Task-2, ITS Task-1): Inform Leadership offboarding procedures for ESM have completed

2 Scope

These policies are applicable for all individuals who are part of Trusted CI.

3 Policy Description

Policy description and justification are noted where appropriate within Section 1. Procedures.

4 Reason for Policy

Trusted CI is now a nationally recognized organization in the NSF science community, hence, not only is it imperative that we *lead by example* in having policy for onboarding/offboarding, but in experiencing sufficient turnover due to our growth, procedures and policies are warranted in order to mitigate against issues exposed in our growth.

4.1 Ticket System

Trusted CI uses a 'ticket system' based on RT to track the various tasks required in the onboarding/offboarding procedures. Only select personnel within Trusted CI need to have accounts on the RT system, and of those, even less are given administrative access. The latter are the only personnel that actually need to log into the system, as others can simply manipulate the system through email. Additional information on our ticket system can be found in the ASAPS.

5 Change Log

Date	**Description of Change**	**Version Number**
Oct 8, 2020	Initial draft	V0.9
Nov 5, 2020	Procedures updated with roles & dependencies	V0.91
Jan 5, 2021	Procedures were moved up into Section 1; final comments addressed	v1.0
May 4, 2021	Added additional mailing lists; changed procedures to account for no SUPV during an offboarding event	v1.1