Master Information Security Policy & Procedures

Trusted CI

Last reviewed on October 5, 2020 by the ISO
Version 2.0

Distribution: Public

Authors: Andrew Adams (CISO), Mark Krenz (CISO), Redacted-For-Privacy (Security Officer), Redacted-For-Privacy (Security Officer)
Chief Information Security Officer: Andrew Adams (security@trustedci.org)
Approved by: Redacted-For-Privacy

Table of Contents

1 Purpose, Scope, and Applicability

This document represents the core cybersecurity / information security policies for Trusted CI, including programmatic commitments, roles and responsibilities, and references to other special purpose policies. Its development was guided by the Trusted CI Framework (see Section 2.1). The Trusted CI Framework outlines 16 "Musts" to help an organization develop its cybersecurity program.

"Cybersecurity" is defined in Appendix B, and is used interchangeably with "information security" in this policy and for the purposes of the cybersecurity program.

This policy applies to all Trusted CI personnel.

Must 1:

Organizations must tailor their cybersecurity program to the organization's mission (**Mission Focus**).

Our information security program is a structured approach to develop, implement, and maintain an organizational environment conducive to appropriate information security and levels of information-related risk. The mission of Trusted CI is:

"To lead in the development of an NSF CybersecurityEcosystem with the workforce, knowledge, processes, and cyberinfrastructure that enables trustworthy science and NSF's vision of a nation that is a global leaderin research and innovation. "

Thus, our cybersecurity program focuses on "collaboration with academia," and it ensures that trust in that process is paramount. Securing our assets (e.g., our SquareSpace account), although highly important, is secondary to fulfilling our collaborative mission. Moreover, since Trusted CI is collaborative in nature, i.e., consisting of personnel from IU, NCSA, PSC, WISC, LBNL, etc., and that it utilizes significant resources from CACR at IU, some policies and procedures are inherited from IU. Albeit, we may choose to modify said inherited policies with our own, and in such a case our own version supersedes IU's.

Must 2:

Organizations must identify and account for **cybersecurity stakeholders**[1] and **requirements**.

Trusted CI Leadership periodically communicates with external stakeholders, e.g., NSF program officer, Leadership at CACR, IU, NSCA, PSC, WISC, LNBL, and Internet2, and discusses this cybersecurity program, its mission and any necessary alterations.

[1] https://drive.google.com/file/d/19E98fENhUNArkXHEKwAExt2wJZna6PIJ/view

In the following sections the components, technologies, policies and processes we prescribe to facilitate our mission in a secure manner are presented.

2 Programmatics

This section describes policy and procedures that govern our cybersecurity program. For more information on the cybersecurity program see https://www.trustedci.org/cybersecurity-program. General information about Trusted CI can be found at https://trustedci.org/.

2.1 Framework

Trusted CI's cybersecurity program is based on the Trusted CI Framework (https://trustedci.org/framework). The Trusted CI Framework (henceforth, Framework) is more flexible than, e.g., NIST's RMF, and thus, better suited for academic-based NSF projects like Trusted CI.

The Framework lays out 16 "Musts" that are essential for a cybersecurity program.

Must 3:

Organizations must establish and maintain **documentation of information assets**

One of the initial steps during the implementation and maintenance of our program is to identify Trusted CI assets. Through systematic polling of personnel, resources that Trusted CI utilized are recorded, along with ownership and expected access control policies. These assets are documented within our Asset-Specific Access and Privilege Specification (ASAPS) folder which resides within the 'Internal Facing Policy & Guidance' within Trusted CI's G Drive 'Mgmt / Internal'.

Must 4:

Organizations must establish and implement a **structure for classifying** information assets as they relate to the organization's mission.

To ensure that our ASAPS documents are consistent, information assets within must be classified using Trusted CI's Information Classification Policy.

Must 8:

Organizations must ensure the cybersecurity program **extends to all entities** with access to, control over, or authority over information assets.

Part of the process in developing an ASAPS document is to ensure that the owner(s) and others

with privileges over that asset are not only recorded in the document, but are contacted and made aware of the authority they possess over that asset.

2.2 Baseline Control Set

Must 15:

Organizations must adopt and utilize a baseline control set.

Trusted CI has adopted the CIS Controls v7.1 as our baseline control set. Specific details regarding the status and application of these controls, and how they associate to our list of documented assets, can be found by using our CIS 7.1 Tracking Tool.

Must 14:

Organizations must identify **external cybersecurity resources** to support the cybersecurity program.

To further ensure both the integrity and confidentiality of Trusted CI's Google Drive service, the ISO (through CACR) periodically runs the Cloudperm tool[2] over Trusted CI's G Drive using a VM owned by CACR. The ISO (through CACR) periodically runs a tool called google-drive-ocamlfuse[3] to perform an offline backup of Trusted CI's Google Drive files. IU also provides the mailing list services that Trusted CI uses, as well as IU's HR and other departments for managing Trusted CI's grants. Moreover, the ISO has requested scans of iso.trustedci.org (ticket system in AWS) from the DorkBot service at UT.

Must 16:

Organizations must select and deploy **additional and alternate controls** as warranted.

At this time, there do not appear to be any additional controls needed based on the assets identified and documented within our ASAPS folder (see Section 2.1). Similarly, there have been no external obligations imposed on Trusted CI (e.g., CUI, CMMC, etc.) that warrant specific additional control sets.

Alternate controls may be required in the future to address risk and-or provide for exceptions to policy, however, these processes are handled during evaluations of our cybersecurity program (see Section 2.5 and Section 2.6).

[2] https://github.com/deltaray/cloudperm
[3] https://github.com/astrada/google-drive-ocamlfuse

2.3 Policy Development, Adoption, and Education

Must 5:
Organizations must involve **leadership** in cybersecurity decision making.

The Information Security Office (ISO, see Section 3.2) is responsible for developing and maintaining cybersecurity policies, and is the first point of contact for any request for clarification of Trusted CI information security policy and-or procedures.

New policies (developed by the ISO) are presented to Leadership for final approval; this process includes potential changes that Leadership may require. If Leadership authorizes the policy, the document is placed in the sub-subfolder 'Security Program Policies' within the Trusted CI G-Drive folder 'Active Policy Documents', which itself is within 'Internal Facing Policy and Guidance' in 'Mgmt / Internal', and all personnel are notified such that they can familiarize themselves with the new/updated policy. If the policy is sufficiently complex, the ISO will provide a presentation at either the annual face-to-face or monthly all-hands-meeting to provide training on the policy to staff.

Changes to existing information security policy are also undertaken by the ISO. Requests for changes to established procedures, if not initiated by the ISO, should be presented to the ISO who will analyze the feasibility and cost of changing the policy and-or procedure. The ISO will also collaborate with the staff responsible for implementing the recommended change and solicit approval by Leadership before making the change, unless an emergency warrants a more immediate change. In the event of the latter, the ISO will inform Leadership promptly as to the impetus/reasoning. Once the policy is updated, the ISO will update staff accordingly.

In adoption of the security program, and in the event of an incident, the ISO will coordinate information security incident response according to Trusted CI's Incident Response policy. Similarly, the ISO will keep Leadership informed regarding security maintenance (e.g., results of scans over Google Drive), either during Trusted CI's Leadership calls and-or Trusted CI's annual face-to-face all-hands meeting.

2.4 Policy Enforcement

Violations of Trusted CI cybersecurity policies can result in loss of access to resources and services and/or disciplinary action. Activities in violation of any laws may be reported to the law enforcement authorities for investigation and prosecution. Anyone who believes that there is a violation of a cybersecurity policy or has a related question should contact: security@trustedci.org.

2.5 Policy Exceptions

Although great care is taken to ensure that Trusted CI policies are not overly burdensome, in some

cases it may be necessary to bypass part or all of a policy. In such an event, the requester must inform the ISO of their need by sending their request to: security@trustedci.org.

The ISO will discuss the exemption with Leadership and inform the requester of the status of the request. Any approved exceptions are noted in the 'ChangeLog' of the appropriate policy, and if the exemption is finite, an ISO ticket is added to the ticket system to alert upon expiration of the exemption.

2.6 Programmatic Evaluation

Must 9:

Organizations must develop, adopt, explain, follow, enforce, and revise cybersecurity **policy**.

Must 10:

Organizations must **evaluate** and refine their cybersecurity program.

The ISO will perform annual reviews of Trusted CI's security program. The reviews will include, but are not limited to: checking the relevance of assets recorded in our ASAPS sub-folder within the 'Information Security Program' folder in 'Mgmt / Internal' and determining if any asset documents need to be removed or added; evaluating the owner, access control and other meta-data regarding each of the existing (and relevant) previously said assets; evaluating the controls applied to each said asset; checking each active information security policy within the 'Internal Facing Policy and Guidance' (see Section 2.3) for relevance and evaluating relevant policies' contents.

If additions and-or changes are made to any document (or control), the appropriate personnel are contacted and informed (see approval and contact steps in Section 2.1 & 2.3).

The periodic annual review is recorded (and alerted from) Trusted CI's information security ticket system (iso.trustedci.org).

External stakeholders, if desiring /needing to add/update policy and-or controls within this cybersecurity program, should contact/pass-through Leadership, and if approved, passed on to the ISO as specified in Section 2.3.

Must 11:

Organizations must devote **adequate resources** to mitigate cybersecurity risks deemed unacceptable by the organization.

Must 12:

Organizations must establish and maintain a cybersecurity **budget**.

Finally, the ISO will report to Leadership at the end of the year what tasks are expected to be required to support and maintain the cybersecurity program, and suggest, in terms of effort allocation -- identified as a percentage of an FTE of the subset of a personnel's allotted Trusted CI time -- appropriate resources for the upcoming year. The total aggregate of resources applied to the ISO is currently .45 of an FTE, spread over 4 personnel. We feel 45% of an FTE is needed to complete the outstanding tasks, e.g., a tool to bulk cp files within the cloud and change permissions, as well as overall maintenance to the cybersecurity program. (See ISO Project Plan.)

3 Roles & Responsibilities

This section lists the roles and-or organizational entities with access to, control over, or authority over Trusted CI information assets.

3.1 Senior Leadership

Must 6:

Organizations must formalize roles and responsibilities for cybersecurity **risk acceptance**.

The Trusted CI Director retains responsibility for cybersecurity risk acceptance except where expressly delegated in this policy or other governing documents. The Director, as well as all of Leadership, also influence Trusted CI's cybersecurity program by recommending policy and procedures to the ISO, and having final authority in approving any policy presented by the ISO.

As of the date of publication of this document, TrustedCI Leadership consists of: Von Welch (Director), Jim Basney (Deputy Director and NCSA Site lead), Kathy Benninger (PSC Site lead), Dana Brunson (Co-PI and Internet2 Site lead), Mark Krenz (Senior staff), Barton Miller (Co-PI and U. Wisconsin Site lead), Sean Peisert (LBNL Site lead), Kelli Shute (Executive Director).

3.2 Chief Information Security Officer

Must 7:

Organizations must establish a **lead role** with responsibility to advise and provide services to the organization on cybersecurity matters.

Must 13:

Organizations must allocate **personnel** resources to cybersecurity.

Trusted CI maintains a position of Chief InformationSecurity Officer (CISO) who reports to Trusted CI Leadership. The CISO is responsible for overseeing and coordinating Trusted CI's Information Security Office (ISO). The ISO is tasked with developing, adopting, explaining, enforcing and revising all components of Trusted CI's information security program (see Section 2). Trusted CI's ISO is composed of:

CISO: Andrew Adams (akadams@psc.edu)
Deputy CISO: Mark Krenz (mkrenz@iu.edu)
Information Security Officer: Redacted-For Privacy
Information Security Officer: Redacted-For Privacy

Mark Krenz, as Deputy CISO, has the same authority as Adams (CISO) within Trusted CI.

'security@trustedci.org' expands to the ISO, Trusted CI Director and Deputy Director.

3.3 All Organizational Personnel

Must 8:

Organizations must ensure the cybersecurity program **extends to all entities** with access to, control over, or authority over information assets.

All Trusted CI personnel are responsible for reviewing and respecting cybersecurity policies and procedures including all documents within the 'Information Security Policies' subfolder in the 'Active Policy Documents' folder (see Section 2.3). Moreover, all personnel are further expected to understand what drives these policies, in order to make rational decisions in situations not specifically covered by the detailed procedures.

Specific staff will be assigned roles to govern specific assets. These assets, as well as the staff assigned to manage them, are outlined and described in the associated Asset-Specific Access and Privilege Specification (ASAPS) documents (see Section 2.1). Thus, it is the responsibility of those staff that are assigned asset-management roles to familiarize themselves with those specific documents.

Finally, all personnel are expected to immediately report any known or suspected violations of security procedures, or known or suspected information security incidents to the ISO (security@trustedci.org).

3.4 Third Parties

Since Trusted CI relies on Google Drive to foster its collaborative nature, it is imperative that all users requiring 'create' privileges have a G Suite (Google Workplan) supervisor that can claim ownership of said files. If the external user doesnot have a G Suite supervisor, then IU will provide the user with an 'affiliated' G Suite account (see Google Drive Policy & Procedures).

Additionally, specific external users may need access to other, non-Google Drive assets at various times. It is the responsibility of the Trusted CI staff who owns/manages those assets (as reported in the ASAPS document, see Section 2.1) to ensure that those external users adhere to Trusted CI policy.

Appendix A: Other Policy and Procedure Documents

This Appendix lists all active special purpose cybersecurity policies (and their location if in external documents). It is the intention that this 'master' document remain an authoritative list of active policies and procedures. Thus, in addition to this document, Trusted CI has adopted the following additional policies and procedures:

- Access Control Policy - Defines the resources being protected and the rules that control access to them.
- Asset-Specific Access and Privilege Specification - A collection of documents that detail policy for the following assets; Adobe Connect, Blogger, e-mail lists, DNS, engagement information, internal information, Squarespace, teleconferencing and Twitter. The policy documents are in the 'Security Program Policies' within the 'Active Policy Documents' folder.
- Information Classification Policy - Used to ensure consistency in classification and protection of data.
- Disaster Recovery Policy - Since all Trusted CI informational assets are either stored within the cloud (i.e., Google Drive), or the credentials and/or other meta-data is housed at other service providers (e.g., Twitter), Trusted CI knowingly relies on those providers to secure Trusted CI assets for data-loss-prevention (DLP). However, to additionally mitigate against catastrophic loss (e.g., ransomware) of information within Google Drive, the ISO will run semi-annual backups of all data in Trusted CI's Google Drive accounts. These backups will be kept under physical lock & key at Indiana University. Moreover, information stored on Trusted CI staff's devices are subject to the purchasing or contracting institution's DR policy.
- Personnel Onboarding Checklist - Form to be completed at the beginning of employment that addresses authorizing access to resources, physical space and any organizational assets checked out such as laptops.
- Personnel Exit Checklist - Form to be completed at the end of employment that addresses revoking access to resources, physical space and the return of organizational assets.
- Incident Response Procedures - A pre-defined organized approach to addressing and

managing a security incident.

- Mobile Computing Policy - Trusted CI defers to a staff member's institutional policies regarding information stored on that institution's laptops, computers, tablets and phones. All internal, for approved access only or confidential engagement related Trusted CI data must be encrypted if downloaded from Google Drive and stored on institutional supplied laptops, computers, tablets and phones. If a staff member usestheir personal device, Trusted CI prohibits staff from storing internal, for approved access only or confidential engagement-related information on those devices.
- Password Policy - Trusted CI **requires** that its staff use unique passwords with strong entropy and strongly suggests they follow Google's advice when generating passwords.[4] Furthermore, Trusted CI **requires** all staff accessing engagement assets stored within Google Drive or with ability to configure or post to the Trustedci.org Blog to use Google's two-step verification[5] or institutional two-factor authentication. The ISO maintains records of all Trusted CI staff accounts that have been self-reportedas using Google's two-step verification or institutional two-factor authentication - referred to in these documents as two factor authentication.
- Privacy Policy - Trusted CI adheres to Indiana University's Privacy Policy.
- Training and Awareness Policy - All new personnel are required to be familiar with all Trusted CI active policies, including those within the 'Information Security Program' subfolder. Additionally, as new policies are created, or existing policies are updated, the ISO will use the Face-2-Face and All-Hands-Meetings as venues to explain the new or updated policies..
- Video Conferencing Policy - Personnel should adhere to their institution's best practices for the personnel's home institution.

[4] https://support.google.com/accounts/answer/32040?hl=en
[5] https://support.google.com/accounts/answer/185839

Appendix B: Terms and Acronyms

[Use this as a central location to define terms and acronyms for all information security policies.]

Cybersecurity: "prevention of damage to, protection of, and restoration of computers, electronic communication systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation."[6] This definition is scoped to include information assets beyond traditional IT, and includes operational technology.[7]

***

This document is based in part on
Trusted CI's Master Information Security Policies & Procedures Template, v3.
For template updates, visit trustedci.org/framework.

[6] https://fas.org/irp/offdocs/nspd/nspd-54.pdf.

[7] "Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events." *See* https://www.gartner.com/en/information-technology/glossary/operational-technology-ot