Trusted CI
Incident Response Policy and Procedures

Last Reviewed on May, 13, 2021 by the ISO

Distribution: **Public**

Authors: Information Security Office
Chief Information Security Officer: Andrew Adams
Deputy Chief Information Security Officer: Mark Krenz

Table of Contents

1 Introduction

This document represents the policies and procedures in place for handling information security incidents impacting services and infrastructure of Trusted CI, including publicly accessible services, supporting information and information systems, and infrastructure used by Trusted CI personnel in support of the Trusted CI mission.

For the purpose of this document, an information security incident (henceforth, an “incident”) includes any known or suspected event that compromises or has the potential to compromise any Trusted CI information asset, including computing infrastructure, confidential data, or computing service, as well as flagrant violations of Trusted CI policy by project personnel, staff, or users of externally-facing services. Incidents that do not involve information assets fall outside the scope of this document.

For information regarding violations and enforcement, please refer to the Trusted CI Master Information Security Policies & Procedures located in the ‘Active Policies’ folder.

2 Incident Response Goals

Any process should have prioritized goals in order to guide time-sensitive tactical decisions. For the purposes of Trusted CI incident response, the goals are, in order of decreasing priority:

1. Minimize negative impact from an incident in terms of exposing confidential information, damage to hardware, software, and/or data assets, and damage to Trusted CI reputation.
2. Collect information needed (a) to understand the specific impact the incident had on impacted assets, (b) to prevent future incidents, and (c) when appropriate, to give law enforcement data useful in pursuing investigation of crimes related to the incident.
3. Record all events from the incident, and all steps of the remediation process in a ticketing system (or other efficient manner).
4. Keep Trusted CI leadership informed, and work with Trusted CI’s Director to identify who and-or what is required in the remediation process, e.g., who should contact affected parties, and what should be conveyed.
5. Maintain the operational availability of services and infrastructure to staff and Trusted CI’s community.
6. Develop a final report describing all events and the remediation process. If permissible, the report should be made public.

Trusted CI’s Director may, for any particular incident, request Trusted CI’s ISO (Information Security Office) to adjust the priority of these goals.

3 Preparations In Place

3.1 Roles and Responsibilities

A clear and widely-communicated plan regarding who will be involved in incident response and individuals’ responsibilities is essential to rapid and effective handling of incidents.

The CISO, Deputy CISO, and security officers within Trusted CI's security team make up the Information Security Office (ISO).

The CISO will be responsible for leading an incident response team and communicating with the Director of Trusted CI. The CISO will form the incident response team that will investigate and act on tasks related to the incident. The team, initially comprising the ISO, will be designated at the time of the incident.

The Deputy CISO, who holds the same authority as the CISO, can act in place of the CISO during the remediation process, as needed.

The Director and the Deputy Director of Trusted CI, henceforth Directors, are responsible for guiding the CISO based on information gathered during the response. Additionally, as alluded to in the goal above (see Section 2), the Directors are responsible for overseeing external communications, e.g., who should be notified, what the notification contains, at what points in the investigation notifications should be sent, and by whom the notifications should be sent. Furthermore, the Directors should explicitly convey to staff that they should offer full cooperation if approached by a member of the incident response team in their role during the incident remediation.

Contact information for the CISO, Deputy CISO, security officers, Director & Deputy Director can be found here:

CISO: Andrew K. Adams
Deputy CISO: Mark Krenz
Security Officer: Ishan Abhinit
Security Officer: Shane Filus
Director: Von Welch
Deputy Director: Jim Basney

Phone & email for the above can be obtained via the: Redacted-For-Privacy

3.2 Escalation Paths

The first sign of an incident could derive from staff or an external communique, as Trusted CI only maintains a few automated intrusion detection/integrity checking systems (e.g., CloudPerm).

If staff alert on the incident, the CISO should be notified immediately about it along with all pertinent information pertaining to it. It is the responsibility of the CISO then to keep the Trusted CI Directors informed of the incident. The Directors will be responsible for external communication with the public or clients during an incident.

The ISO will maintain an email address Redacted-For-Privacy, which external parties can use to notify Trusted CI of an incident which impacts Trusted CI assets. This email address will forward to the CISO and deputy CISO. The CISO will form the security-team through phone calls (numbers obtained from the Effort Allocation Sheet). Documents and other similar information can be exchanged in the ISO's private Google Drive folder. If the incident involves Google Drive, the CISO will create a shared key for the purpose of encrypted exchanges in lieu of using Google. Additionally, the CISO will create a separate shared key for future exchanges with external 3rd parties.

Note, under normal circumstances Redacted-For-Privacy is not publicized. We expect external parties to reach out to us through the 'Contact Us' page on our website. We would then give them the Redacted-For-Privacy mailing list for future correspondences.

3.3 Alternate Logging Conventions

If there is concern of a compromise in Trusted CI's Google Drive space, then it should be avoided during the process of recording the incident response and sharing information. The CISO can use discretion on where to record the incident response in that scenario e.g., using a shared GPG symmetric key.

3.3 Incident Response Procedure(s) Testing

Response procedures cannot be considered reliable if they have not been tested. The ISO will conduct, on a monthly basis, security exercises. These exercises are typically table-top exercises within the ISO. Annually, selected staff will also be included to expand upon the scope of the simulated security exercise. Both the security team's internal table-top exercises and the annual extended-scope exercises will be organized by the members of the ISO and potentially include others who could be involved in the incident as needed. The ISO is responsible for setting the theme, time and location of the incident.

3.4 External Documentation

The ISO will maintain the following on an ongoing basis in order to facilitate response to an incident:

- Relevant contact information for secure communication to and between incident response team members during an incident, e.g., phone numbers and GPG keys for email addresses not hosted on Trusted CI infrastructure
- An asset inventory detailing all IT assets along with appropriate Asset-Specific Access and Privilege Specifications (ASAPS)
- Instructions on reporting incidents are to be made available through the "Contact" page on the Trusted CI website at https://trustedci.org/; additionally, if further communications are needed, the list address Redacted-For-Privacy will be given to the external party to communicate directly with the ISO
- An up to date and accessible offline copy of this document and other Trusted CI policies and procedures

4 General Procedures

4.1 Identify

Incidents may be reported by alerts from Trusted CI personnel, Trusted CI engagees, or by other third parties. As mentioned in Section 3.2, alerts sent in via Redacted-For-Privacy will go to the CISO/Deputy CISO, who will then identify the incident. Additional communication may be required to fully identify the incident.

4.2 Assess and Preserve

4.2.1 Initial Triage and Categorization

Trusted CI information security incidents are classified based on their perceived impact. Classification may change as understanding of the incident evolves. The first person to respond to the incident should attempt to give a first-estimate categorization in order to guide response. These classifications of incident prioritization are based on those in [NIST 800-61] Section 3.2.6.

- High: an incident is considered High Severity if it involves:
  - Compromise of information classified as ‘Restricted’
  - Compromise of confidentiality or integrity of PII
  - Compromise of confidentiality or integrity of software vulnerability information
  - Attention to the security incident by media outlets, or other public dissemination (e.g. social media)
  - Major disruption to the project’s ability to provide services to the user community
  - A successful compromise is believed to have been ongoing for more than a week
  - An incident is believed to have possible financial consequences
  - An incident is believed to involve an insider threat
- Medium: an incident is considered Medium Severity if it involves:
  - Compromise of information classified as ‘For Internal Use Only’
  - Any compromise that appears to specifically target Trusted CI assets or personnel
- Low: an incident is considered Low Severity if it involves:
  - A short-term (less than 10 minute) disruption in Trusted CI’s assets due to a denial of service attack
  - A long-term disruption to non-critical services or degradation of critical services
  - Attempted but unsuccessful attempts to compromise Trusted CI’s assets in some way that appears to target the project specifically and is not normal untargeted Internet “background noise”

Based on this initial categorization, the following actions should be taken:

- High Severity: The CISO should contact the primary maintainer of the affected system(s) immediately by phone, and request that any compromised assets be disabled as soon as possible.

- Medium Severity: The CISO should contact the primary maintainer of the affected system(s) immediately by phone during business hours, or email during off-hours, and request that any compromised assets should be disabled.
- Low Severity: The CISO should contact the primary maintainer of the affected system(s) by phone during business hours, and request that any compromised assets should be disabled.

4.2.2 Isolation:

In any incident, it is important to act quickly in order to keep damage from spreading. Before or in parallel with the formation of an incident response team (when required), the CISO/Deputy CISO doing initial triage should take steps, e.g., removing references to embargoed data, to prevent the problem from spreading to other accounts or resources.

4.2.3 Formation of the Incident Response Team

The CISO may form an incident response team. The composition of this team will depend on the nature of the incident (e.g., an administrator of an asset may be called upon if a vulnerability is found in Trusted CI's web server) and may evolve during the incident.

4.2.4 Information Capture

Information capture during an incident is essential to fast and appropriate resolution of the incident, as well as to understanding the incident's cause, working with law enforcement regarding the incident, and doing an effective postmortem. Members of the incident response team should log their actions (on paper if needed to isolate record-keeping from potentially compromised assets), along with times and observations made. Additionally, team members must, whenever possible, keep copies of malicious software found, and other signs of compromise for later analysis.

4.3 Eradicate and Recover

Once the vulnerability/breach has been addressed, where possible, recover compromised assets through backup.

4.4 Notification

The CISO is responsible for keeping the Directors informed during the incident. The Directors will decide who (e.g., stakeholders, impacted engagees, institutional ISO), how, and when to notify. The CISO will assist the Directors in writing the incident response and identifying who should be notified and at what points in the response.

4.5 Follow Up

A thorough postmortem following any incident is essential to the continued improvement of

Trusted CI’s cybersecurity program. Following an incident, documentation created during the incident should be checked for accuracy by the incident response team and detailed to the point that the IR report can be published.

Following an incident, the incident response team should conduct a verbal walk-through and discuss what was done well, and how response procedures can be improved. Additionally, the team should discuss the underlying cause of the incident and propose steps appropriate to prevent similar compromises in the future.

5 Specific Scenarios

This section lists scenarios that require specific or unique actions on behalf of the incident response team. As new services/assets are acquired by Trusted CI, *if* actions needed to mitigate those are different than the below, those actions should be included.

5.1 Staff Google Drive Credential Compromise

Redacted-For-Privacy

5.2 Breach of Restricted Data

Redacted-For-Privacy

5.3 Compromise of Public-facing Services

Redacted-For-Privacy

5.4 Malicious Insider Attack

Redacted-For-Privacy

5.5 Ransomware Attack on Google Drive

Redacted-For-Privacy

6 Change Log

Date	**Description of Change**	**Version**
05/14/2020	Added extensive changes to overhaul old IR policy (too numerous to list)	1.0
08/10/2020	Ensured ‘Contact Us’ web page matched policy, as well as external security alias email	1.1
04/01/2021	Updating redactions	1.2
05/13/2021	Add ‘Version’ to changelog table, fixed dates, additional redactions	1.3

***

This policy is based in part on Trusted CI Incident Response Policy Template, v2. For updates, visit trustedci.org/guide.