

Master Information Security Policy & Procedures  
Center for Trustworthy Scientific Computing (CTSC)

Version 1 - March 2016

Authors: Andrew K. Adams, Mark Krenz, James Marsteller  
Information Security Officer: James Marsteller

# Table of Contents

- [1 Introduction](#)
- [2 Roles & Responsibilities](#)
  - [2.1 Information Security Officer](#)
  - [2.2 Asset Managers](#)
  - [2.3 Project Personnel and Staff](#)
- [3 Developing, Implementing, and Maintaining Our Cybersecurity Program](#)
  - [3.1 Information Security Risk Management Processes](#)
  - [3.2 Enforcement](#)
  - [3.3 Modifications to Information Security Policies and Procedures](#)
- [4 Policy and Procedure](#)
  - [4.1 Disaster Recovery](#)
  - [4.2 Incident Response Policy and Procedures](#)
  - [4.3 Password Policy](#)
  - [4.4 Staff Data Handling](#)
- [5 Other Policy and Procedure Documents](#)

# 1 Introduction

This document represents the core information security policies and procedures for CTSC, including information security-related roles and responsibilities; references to other, special purpose policies; and the core procedures for developing, implementing, and maintaining the information security program.

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. This program entails ongoing activities to address relevant policies and procedures; technology and mitigations; and training and awareness.

## 2 Roles & Responsibilities

### 2.1 Information Security Officer

CTSC maintains a position of Information Security Officer (ISO), who is additionally a PI. The ISO has responsibility for overseeing and coordinating the components of the information security program, and reporting the program's state to CTSC's Leadership Team. The ISO maintains all operative policy and procedure documents, including this document, and will distribute them as appropriate. All reviews of CTSC wide policies and procedures are coordinated and archived through this office. The ISO also documents any changes made to the security policy based on these reviews.

The ISO is the first point of contact for any request for clarification of CTSC information security policy and procedures. The ISO will coordinate information security incident response, including correspondence between the affected staff and users.

As of the date of publication of this document, the Leadership Team consists of Von Welch, Jim Basney, Barton Miller, Craig Jackson and Jim Marsteller, who is also the ISO. In the event of Marsteller being unavailable, Von Welch will serve as the backup ISO or appoint an interim ISO. Contact information for the ISO follows: [security@trustedci.org](mailto:security@trustedci.org)

### 2.2 Asset Managers

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, including: [trustedci.org](http://trustedci.org) website, @TrustedCI twitter account, Adobe Connect service, CTSC mailing lists @IU, teleconferencing services, DNS for [trustedci.org](http://trustedci.org), and [trustedci.org](http://trustedci.org) blog. Thus, it is the responsibility of those staff that are assigned asset-management roles to familiarize themselves with those specific documents.

Additionally, external users, e.g., engagees or NSF officers, may need access to specific assets at various times. It is the responsibility of the CTSC staff who owns/manages those assets to ensure that those external users adhere to the above policy documents as well.

## 2.3 Project Personnel and Staff

It is the responsibility of each individual working for CTSC to review and respect the following policy documents: Access Control Policy, Information Classification Policy and this Master Information Security Policy & Procedures. The staff member is further expected to understand what drives these policies, in order to make rational decisions in situations not specifically covered by the detailed procedures. It is also the staff member's responsibility to review the policies that govern any specific CTSC assets they access (see [2.2 Asset Managers](#)) as well as the ASAPS for information assets, approved access only information assets and internal information assets.

Each staff member or external user is expected immediately to report any known or suspected violations of security procedures, or known or suspected information security incidents to the ISO ([security@trustedci.org](mailto:security@trustedci.org)) or project leadership. In all cases, the staff member or external user and the time of the incident will be documented in order to support a timely analysis of and coordinated response to the situation.

# 3 Developing, Implementing, and Maintaining Our Cybersecurity Program

## 3.1 Information Security Risk Management Processes

There are many frameworks that we evaluated over the years but none are tailored specifically for NSF funded projects. In 2014 CTSC released "Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects" that was influenced by many industry recognized approaches to risk management including the National Institute of Standards and Technology (NIST). We believe the CTSC guide provides the best guidance on cybersecurity challenges faced by the scientific community and therefore we selected it as the basis for our cybersecurity program. As a beginning point, CTSC developed an [Information Asset Inventory](#) in order to itemize all of its resources. The asset inventory, along with associated vulnerabilities and the potential threats via those vulnerabilities to the assets was then used to identifying risk in the [Risk Assessment Table](#).

## 3.2 Enforcement

Violations of CTSC information security 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 proper authorities for investigation and prosecution. Anyone who believes that there is a violation of any information security policy or has a related question should contact: [security@trustedci.org](mailto:security@trustedci.org)

### 3.3 Modifications to Information Security Policies and Procedures

The Information Security Officer (ISO) is responsible for coordinating changes to established policies and procedures. Requests for changes to established procedures should be presented to the ISO who will analyze the feasibility and the cost of changing the procedure. The ISO will also collaborate with the staff responsible for implementing the recommended change and solicit approval by the leadership team before making a change, unless an emergency warrants a more immediate change. The ISO, with approval from the leadership team, approves all internal changes to policies and procedures and will update staff accordingly.

## 4 General Policies and Procedures

This section covers specific policy and procedures for CTSC assets that are sufficiently tractable to not warrant a policy document unto themselves.

### 4.1 Disaster Recovery

Since all CTSC 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), CTSC knowingly relies on those providers to secure CTSC assets against disaster. However, to additionally mitigate against catastrophic loss (e.g., ransomware) of information within Google Drive, the info-sec staff will run semi-annual backups of all data in CTSC's Google Drive accounts. These backups will be kept under physical lock & key at Indiana University.

Information stored on CTSC staff's devices are subject to the purchasing or contracting institution's DR policy.

### 4.2 Incident Response Policy and Procedures

An accident or malicious incident that causes a violation of any of the policies in this document, or otherwise threatens CTSC activities or public-facing services, should be reported to the CTSC ISO. The CTSC ISO will coordinate response to the incident.

The priorities of CTSC Incident Response will be:

1. Minimize loss of confidentiality of CTSC sensitive and engagement-related documents.
2. Understand the scope of any loss of confidentiality, integrity or availability.
3. Restore CTSC activities to normal.

## 4.3 Password Policy

CTSC requires that its staff use unique passwords with strong entropy and strongly suggests they follow Google's advice when generating passwords.<sup>1</sup> Furthermore, CTSC 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<sup>2</sup>. The ISO maintains records of all CTSC staff accounts that have been self-reported as using Google's two-step verification - referred to in these documents as two factor authentication.

## 4.4 Staff Data Handling

CTSC 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 CTSC data must be encrypted if downloaded from Google Drive and stored on institutional supplied laptops, computers, tablets and phones . If a staff member uses their personal device, CTSC prohibits staff from storing internal, for approved access only or confidential engagement-related information on those devices.

# 5 Other Policy and Procedure Documents

In addition to this Master document, CTSC 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.
- Information Classification Policy - Used to ensure consistency in classification and protection of data.
- Information Asset Inventory - An Itemized list of CTSC resources.
- Risk Assessment Spreadsheet - Matrix used in calculating inherent risk to each of CTSC's assets.

\*\*\*

*This document is based in part on  
CTSC's Master Information Security Policies & Procedures Template, v2.  
For template updates, visit [trustedci.org/guide](http://trustedci.org/guide).*

---

<sup>1</sup> <https://support.google.com/accounts/answer/32040?hl=en>

<sup>2</sup> <https://support.google.com/accounts/answer/185839>