

Information Asset Inventory  
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

## [Introduction](#)

### [1 Information Inventory](#)

[Information is any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.](#)

#### [1.1 Type of Information](#)

### [2 Information Systems Inventory](#)

[An information system is a discrete set of information and related resources \(such as people, equipment, and information technology\) organized for the collection, processing, maintenance, use, sharing, dissemination, and/or disposition of information.](#)

#### [2.1 Type of Information System](#)

# Introduction

This document represents CTSC’s authoritative inventory of information assets (i.e., information and information systems) as of the version date for the purposes of information security. Section 1 contains an inventory of CTSC’s information organized by information type. Section 2 contains an inventory of information systems. Both Sections 1 and 2 contain summary information regarding the security objectives (confidentiality, integrity, availability) relevant to each asset or type of asset. Section 3 provides additional descriptive details regarding key information assets. Section 4 contains listings of related resources and helpful figures.

Unlike policy documents, which may be reviewed infrequently, this inventory must be kept extremely up to date to remain relevant and useful. Ideally, it should be updated every time there is a change in any of the information listed or the [Risk Assessment Table](#). This has proven to be lower-overhead than doing a monthly or quarterly inventory to update the documentation.

For information regarding violations and enforcement, please refer to the CTSC Master Information Security Policies & Procedures located at <http://trustedci.org/cybersecurity-program/>

## 1 Information Inventory

*Information* is any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

### 1.1 Type of Information

⇒ Enter a description of this information type here. It should be specific enough that someone who was handed a disk full of data can easily determine whether the data they have belongs to this classification or not. In the table below, you’ll list information that’s part of this set.

Asset Name	Short Description	Owner	Asset Detail
Public Information / Tools	Information is not confidential and can be made public without any adverse implications.	Pls, Data asset	See the “CTSC Information

		manager(s)	Classification Policy")
Engagement-related Information	This information can only be accessed and modified by CTSC staff who have implemented 2FA, and participating engagee staff.	Engagement Leads	See the "CTSC Information Classification Policy"
Internal Information	Information collected and used by CTSC in conducting its work. Access to this information is governed by CTSC's ISO and PIs and is restricted to CTSC staff.	PIs	See the "CTSC Information Classification Policy"
For Approved Access Only	Information is restricted to specified individuals or classes or roles, approved by CTSC's ISO, PIs or engagement leads.	PIs	See the "CTSC Information Classification Policy"

CTSC's documents have the following requirements for:

**Confidentiality:** Internal documents must remain confidential. Unless noted otherwise, engagement-related documents additionally need to be kept confidential within the set of defined principles involved.

**Integrity:** The integrity of all documents are critical, both for our continued operation, as well as an archive of our foundations and achievements.

**Availability:** While availability of all data is important, none needs to be accessible at all times. Permanent loss of any of the data, especially the engagement-related and public information, would be prove to be costly and potentially embarrassing.

## 2 Information Systems Inventory

An *information system* is a discrete set of information and related resources (such as people, equipment, and information technology)

organized for the collection, processing, maintenance, use, sharing, dissemination, and/or disposition of information.

## 2.1 Type of Information System

⇒ Enter a description of this system type here. It should be specific enough that someone who was handed a disk full of data can easily determine whether the data they have belongs to this classification or not. In the table below, you'll list information that's part of this set.

Asset Name	Short Description	Owner	Asset Detail
TrustedCI Web Front-end	Our web-based interface to the public, containing links to documents within our Google Drive, as well as contact information	See related ASAPSTrustedci.org Website	ASAPS, Risk Assessment Matrix
Blog	blogger.com(google)	See CTSC ASAPS - Trustedci.org Blog	ASAPS, Risk Assessment Matrix
Twitter identity		See CTSC ASAPS - @Trustedci Twitter account	ASAPS, Risk Assessment Matrix
Ghandi.Net Service	Domain name services	See CTSC ASAPS - DNS for trustedci.org	ASAPS, Risk Assessment Matrix
Adobe Connect	Webinar	See CTSC ASAPS -	ASAPS, Risk Assessment

		Adobe Connect service	Matrix
IU mailing lists ( <a href="mailto:team@trustedci.org">team@trustedci.org</a> , announce lists)		See CTSC ASAPS - CTSC mailing lists at Indiana University	ASAPS, Risk Assessment Matrix
Teleconferencing services		See CTSC ASAPS - Teleconferencing services	ASAPS, Risk Assessment Matrix
Backup Device for Google Drive documents	This is a thumb drive that is kept in a locked safe at the secure offices of CACR on the IU Bloomington campus.	Mark Krenz	Master Information Security Policy & Procedures

**Confidentiality:** The Google Drive backup device must remain confidential, as it holds types of information from Internal, Engagement-related and For Approved Access Only.

**Integrity:** All systems must ensure that all types of information remain unchanged.

**Availability:** All systems should remain operational for all types of information. The Google Drive backup device must remain available.

\*\*\*

*This document is based in part on CTSC Information Asset Template, v2.  
For template updates, visit [trustedci.org/guide](http://trustedci.org/guide).*