Access Control Policy
Center for Trustworthy Scientific Computing (CTSC)

Version 1.0 / March 2016

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

Table of Contents

1 Introduction

Access control is fundamental to information security and represents the organization's policies and practices around who has access to what information and information systems, the extent of that access (i.e., level of privilege), and when and under what conditions that access is granted and revoked. This document is a high level statement of CTSC's mandatory access control policies and core procedures.

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

2 General & Default Access Control Policies Procedures

CTSC's goal is to limit access to information and information systems to authorized users, and processes acting on behalf of authorized users; and to limit that access to appropriate levels of privilege.

The following policies and procedures apply to all CTSC's information and information systems, notwithstanding specific asset-based requirements stated in Section 4.

2.1 Granting Access and Privileges

In general, CTSC subscribes to a "least privilege" approach to access control, specifically that a person be given the lowest level of access and privileges required for that person to do interact with that information or information system appropriately and efficiently.

Unless stated otherwise for a particular asset, the CTSC Information Security Officer has ultimate authority to authorize and revoke access of individuals, classes of individuals, or other organizations to CTSC's information and information systems. The Information Security Officer may expressly delegate this authority.

2.2 Documenting Access and Privileges

The people for whom the CTSC controls access are divided into the following general categories:

- **The Public**
- **CTSC PIs**
- **CTSC PIs and selected staff**
- **CTSC Staff -** This includes staff members of the CTSC project.
- **CTSC Staff and engagement personnel -** CTSC staff and staff from a projects we are cooperating with on an engagement, as well as anyone else the engagees designate to have access to information related to their engagement.
- **CTSC Asset Managers -** Staff members designated with responsibilities for managing

specific asset-related content.

2.3 Reviewing Access and Privileges

Unless stated otherwise for a particular asset, the Information Security Officer (ISO) will review the state of access control documentation and correctness of the implementation on a semiannual basis.

2.4 Revoking Access and Privileges

Unless stated otherwise for a particular asset, access and privileges for CTSC's information and information systems must be revoked within 24 hours of any person becoming ineligible.

When personnel are to be involuntarily terminated for any reason, all access and privileges should be revoked prior to notice of termination or, if this is impracticable, as shortly thereafter as is feasible.

Checklist for revoking access:

1. Change ownership of any documents in Google Drive to the (new) asset manager or engagement lead.
2. Remove view/edit access to all documents in Google Drive.
3. Unsubscribe person from CTSC controlled mailing lists.
4. Change any shared passwords the the person had access to for specific CTSC resources such as the trustedci.org website, DNS, Twitter, etc.
5. Notify all CTSC staff of personnel change.

3 Asset-Specific Access and Privilege Policies and Procedures

The following is a list of information assets for which there are more specific access and privilege requirements, and the location and/or procedures for obtaining that documentation. Where the requirements are more highly specified for a particular asset, they supersede the general, default requirements in Section 2 above. For each asset, there is a corresponding asset-specific access privilege specification document located in the CTSC Information Security Program folder, each with the document name prefix of ASAPS. These documents are categorized as internal information.

3.1 Google Drive stored information assets

The CTSC has information assets stored in Google Drive that fall into 4 general categories (see CTSC Information Classification Policy) for access control. See CTSC Information Asset Inventory for a description of these categories. In addition to these categories we have specific information assets handled separately. For each category, we require different access controls as follows.

- **Public information -** Anyone can access this information but it does not have to be public accessible. Selected CTSC staff can modify the information.

- **Engagement related information -** This information can only be accessed and modified by CTSC staff and individuals involved in the specific engagement related to the information. CTSC Staff with access to this information must use two factor authentication on their accounts.
- **Approved Access Only information -** This information can only be accessed and modified by CTSC staff as needed. Access to this information also requires two factor authentication.
- **Internal information** - This information can only be accessed and modified by CTSC staff.

3.2 Other specific information Assets

- **trustedci.org web site-** Anyone can access this information. Only specific CTSC staff have access to modify this information
- **blog.trustedci.org -** Anyone can access this information. Only select CTSC staff have access to modify this information or make a post. Ability to post requires two factor authentication.
- **blog.trustedci.org comments -** Anyone can post a comment to a blog entry, but it must be approved by the CTSC Webmaster or other designated CTSC staff.
- **Mailing lists hosted at Indiana University -** Most lists are open and subscribers can post to these mailing lists and access the list archives. Some internal lists require additions to the list by the list owner(s). Only select CTSC PIs and CTSC staff may make changes to the mailing list configuration or add new mailing lists.
- **“TrustedCI” Twitter account -** The public may view posts to this account and subscribe to it without authorization or approval. Only select CTSC staff can make posts to this account.
- **DNS -** Only the protected CACR account and selected CTSC staff may make changes to the DNS configuration for the trustedci.org domain.
- **Teleconferencing services -** Only selected CTSC PIs and CTSC staff may make changes to the teleconferencing service configuration.
- **Adobe Connect -** Only select CTSC PIs and CTSC staff may make changes to Adobe Connect configuration.

***

This document is based in part on CTSC Access Control Policy Template, v2.
For updates, visit trustedci.org/guide.