Information Classification Policy
Center for Trustworthy Scientific Computing (CTSC)
Version 1 - March 2016

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

CTSC has adopted this information classification policy to support the management and protection of information, including electronic data.

- Asset managers are responsible for assigning classifications to information assets according the standard categories presented below.
- Wherever possible, the information category shall be embedded in and visible on the information itself.
- All CTSC personnel shall be guided by the information category in their security-related handling of CTSC information.

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

All CTSC information and all information entrusted to CTSC by third parties falls into one of the classification categories in the following table. These categories are presented in order of increasing sensitivity.

Information Category	**Description**	**Examples**
Public / Unrestricted	Information is not confidential and can be made public without any adverse implications.	● Information widely available in the public domain or for which wide distribution is desirable, e.g., published research results. ● @TrustedCI Twitter content. ● Trustedci.blog content. ● Trustedci.org web content. ● CTSC's cybersecurity policies and procedures.
Engagement-related information	This information can only be accessed and modified by CTSC staff who have implemented 2FA, and participating engagee staff.	● Engagement related documents, policies, project plans, networking diagrams, meeting notes.
Internal Access Only	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.	● Personal (as opposed to office) contact information for project personnel. ● Information about participants in public events. ● Pre-publication research data and CTSC engagement information/reports while

		under development before being shared with engagee.
For Approved Access Only	Information is restricted to specified individuals or classes or roles, approved by CTSC's ISO, PIs or engagement leads.	● User passwords. ● Personnel data. ● Information under NDA. ● DNS Configuration. ● Trustedci.org web configuration and ability to post content. ● Trustedci.org blog configuration and ability to post content. ● @TrustedCI Twitter account configuration and ability to post content. ● Teleconferencing system configuration and scheduling. ● Information with heightened security requirements defined by engagee.

This document is based in part on CTSC Information Classification Policy Templates, v2.
For template updates, visit trustedci.org/guide.