



CIO-100: Information Technology – 29 January 2023

Purpose

The Information Technology (IT) team is responsible for the INCOSE technical infrastructure, web site, “Connect” collaboration area, membership management system, email, webinar and conference facilities and all related information handling resources.

Applicability

This policy applies to the support and use of IT resources by all INCOSE members and guests

Definitions

None

Policy Content

The charter of the Information Technology team is as follows:

- To help INCOSE be recognized as the definitive source for systems engineering information by making it available and accessible;
- To ensure that an effective and high-quality collaboration infrastructure is available to current and potential corporate and individual members as well as the larger community and general public;
- To support sales and distribution of materials from the Publications Office;
- To support targeted INCOSE initiatives; and
- To maintain an archive of INCOSE materials.

In pursuit of this goal:

1. The CIO shall develop and maintain the IT portions of the INCOSE annual operating and long-range plans.
2. The CIO and IT Team shall be responsible for writing and maintaining practices related to use of information technologies. Information technology practices involving a subset of INCOSE committees and working groups shall be coordinated with representatives of the affected groups.



3. The CIO and the IT function shall create and maintain an IT infrastructure that supports communication and collaboration. This shall include services such as, a website accessible to non-members, a web-enabled site accessible to members-only, membership management software, online INCOSE Product Store and product access capabilities, coordination of a membership e-mail distribution mechanism and other collaboration services.
4. The CIO shall maintain and provide means for access to an IT infrastructure that supports an archive of historical and active INCOSE documentation. The Operations Manager is responsible for the storage and access of hard-copy documentation and the archive of physical media.
5. In accordance with good IT internal security practice, all key INCOSE information, draft work products, completed work products, presentations and documents (herein referred to as “INCOSE work”) will be stored in INCOSE systems. INCOSE systems include the INCOSE email system (using Microsoft Exchange and Outlook), Microsoft Teams, Yammer, SharePoint, and OneDrive. INCOSE work may also be stored on personal and work computers, but a current copy should always be maintained on INCOSE systems (see related policies in COM-100 regarding the use of INCOSE email systems).
6. Those who maintain INCOSE information systems (and thus have admin rights to the systems) including the CIO, staff, employees, contractors, directors, and volunteers shall maintain information in accordance with the wishes and direction of those managing the information. Those with admin access to systems will only access information or modify systems under the direction of those who manage the information based on their role. For example, admins may not add themselves or anyone else to a Team or Yammer community without the owner’s explicit permission and may not access information in a Team of which they are not a member. Admins who assist users by creating Teams, Groups, or other information repositories (and thus are owners initially), will retrain the owner role only until the repository is established and then will remove themselves from the group, unless otherwise requested by the group’s owner.
7. Information access within INCOSE is based on reasonable need. For example, the INCOSE membership function will have access to membership information and the INCOSE Marcom function will have access to marketing materials, campaigns, messages and social media posts, regardless of who created the information.
8. Accounts created on outside systems used by INCOSE (such as Zoom, Vimeo, Smartsheet, etc.) will be established using an INCOSE email address, such as cio@incose.net or john.doe@incose.net (or any other INCOSE-owned domain) so that INCOSE maintains ultimate control over these accounts.



9. It is natural for leaders in INCOSE to maintain lists of people in the groups they manage or support. Such lists must be maintained in accordance with good IT security and privacy policies, should contain only the information needed, and should be subject to the opt-in requests of those on the list (such as those who have chosen to join an INCOSE group). Opt-out and removal requests must be honored. Lists must be protected and not released to anyone for commercial or personal use outside of INCOSE.

The Information Technology Team is led by the Chief Information Officer (CIO), who is elected to the Board of Directors per the Bylaws and Policy BOD-100. The Director is supported by Assistant Directors as required. The Assistant Directors serve for two (2) years. There is no term limit for Assistant Directors, but the selection and approval shall be reconfirmed every two (2) years at a minimum.

The IT Team may also be supplemented by paid contracted resources as required and budgeted, to meet the needs of specialized or extended demands upon the IT solutions offered to the membership.

Charter

SUPERSEDES: CIO-100 dated 29 Nov 22

APPROVED BY: INCOSE Board of Directors, Q1 BoD Meeting, Torrance CA, 29 January 2023

MAINTAINED BY: (RACI Responsible R): Chief Information Officer

POLICY OWNER: (RACI Accountable A): President-Elect