BYU HAWAII

Church Educational System
Security Operations Center

Information Technology Security Council Charter

Last Updated: 5 August 2025

Document Custodian: John Payne
Chief Information Security Officer
801-422-9099
John_Payne@byu.edu

Role

The Information Technology Security Council (ITSC) is established to ensure that the University's information assets and technologies are adequately protected against threats, vulnerabilities, and misconfigurations in conjunction with the CES Security Operations Center (CES SOC). The ITSC is focused on creating a local campus security roadmap that complements the CES security roadmap, services, standards, projects, and initiatives (avoiding duplication of solutions or services) to assess, measure, prioritize, report, mitigate, and resolve IT security risk. The primary role of this council is to take active steps to mitigate IT security risk campus wide.

Responsibilities

The primary responsibilities of the ITSC are as follows:

- **Risk Management**: Proactively assess and measure IT security risk for campus IT systems and services, recording and prioritizing those risks in the risk register, with regular review. Report on IT security risk to OIT leadership and the CES CISO. Work with the broader campus IT community to mitigate and resolve IT security risk. Maintain a local campus security roadmap to address security risks that aren't immediately mitigated or resolved.
- **IT Standards Development**: Guide the development, documentation, and implementation of IT Standards for the BYU-Hawaii campus. IT Standards for the campus should start with standards set by the CES Security program and include focus areas that are unique or specific to the campus. Documentation associated with this effort should include technical security procedures that guide the "how to" of the implementation of IT security standards and requirements.
- **IT Security Incident Response**: Assist with information security post-incident response and remediation efforts as needed. As security incidents perform lessons learned activities and identify ongoing risk items, those items are given to this council for ongoing remediation and resolution activities.
- **Collaboration**: Facilitate collaboration among university departments, researchers, the CES SOC and others affiliated with the University to address IT security challenges and opportunities.
- **Compliance and Assessment**: Assist with addressing IT compliance needs for regulations and standards such as HIPPA, FERPA, PCI, and GLBA (Gramm-Leech-Bliley Act). Participate in IT portions of campus audits and assessments.
- **Other Assignments**: Fulfill other assignments given by the CIO, OIT leadership, and CES CISO.

Reporting

Report directly to OIT leadership and the CES CISO at least semi-annually and more often as needed. Reports can include an overview of key activities, risk issues, recommendations for improvement, and a measure of risk mitigation and reduction the council has accomplished.

Meetings

The ITSC meets bi-weekly. The council chair manages the meeting agenda, invites others to attend as needed, etc.

In the absence of specific agenda items, the council should continue to meet to focus on assessment, measurement, and prioritization of IT security risk. Meetings are typically held online to enable full participation of remote participants.

Membership

Membership of the ITSC currently consists of the following:

- Todd Brown, IT Security Risk Manager - CES SOC (Chair)
- Darryl Kimak
- David Te'o
- Arley Enesa
- Jeremy Wright
- Crimson Castillo
- Maae Taala
- Jared Mariano
- Frank Kalama
- Jared Nikora
- Mark Longhurst – CES Network Center
- Other invitees as needed.

Membership is reviewed by the CES Leadership team and the CES CISO annually, with input from the council chair about missing skillsets, participation of existing members, etc. (Last review of membership – August 2025)