

CES Information Security Program & CES Security Operations Center Charter

Church Educational System
Security Operations Center

Last Updated: 23 May 2025

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

Purpose

The CES Information Security Program and CES Security Operations Center (CES SOC) exist to protect the nonpublic institutional data of BYU, BYU-Hawaii, BYU-Idaho, and Ensign College. The information security program takes a measured, risk-based approach towards defining and implementing security capabilities, priorities, policies, and practices. Alignment of strategic vision, priorities, technology, and operations for cybersecurity is performed in a consistent and collaborative manner across campuses to provide a level of assurance, reduce costs, and ensure adequate protections for all schools.

As a partner to each campus, the CES SOC provides cybersecurity services that will help safeguard IT assets, sensitive data, and people. The CES SOC focuses on four primary priorities:

- Deterrence of cybersecurity attacks (protection against without a guarantee of stopping all attacks) with effective use of technology, education, and awareness
- Timely response to and resolution of cybersecurity attacks to limit financial, legal, privacy, and reputational risk and exposure
- Early detection of cyber intrusions through automated security monitoring tools and proactive threat hunting
- Assessment, measurement, and reporting of IT security risk

Personnel

The CES Chief Information Security Officer (CISO) is a BYU employee reporting to the CES/BYU CIO who serves as the local CISO for each campus, working with campus CIOs.

The CES SOC is led by a CES SOC Director with nine full-time and twelve part-time (BYU student) employees. They are BYU employees, are physically located on the BYU campus, and are available to periodically travel to the campuses to ensure needs are being met effectively.

CES CISO

John Payne
801-422-9099
John_Payne@byu.edu

CES SOC Director

Kaylee Hill
801-422-6961
Kaylee.Hill@byu.edu

Responsibilities

The CES CISO oversees the implementation and improvement of the CES information security program, governed by the CES Commissioner's Office and CES IT Leadership.

The CES SOC is organized into six primary operational pillars. For details, see <https://ces-ciso.byu.edu/> (Authentication required)

Additional (non-dedicated) staff at BYU supports security architecture, security engineering, user awareness, and other security related activities in support of the CES information security program and CES SOC.

Measurement

The CES CISO provides regular (at least annual) updates to local campus executives about the state of the information security program, ongoing IT security risk, measurements, and ongoing priorities for improvement.

The CES Information Security Program and CES SOC provides regular measurements and reports about local campus or individual unit risk, the activities and effectiveness of the CES SOC pillars, security protections, attacker activity, etc. For details, see the CES Information Security Program document listed below.

Interaction with the campuses

The CES SOC works directly with local IT staff as partners of those organizations and should be seen as an extension of each campus' IT resources. CES SOC staff may be members of local IT committees, work groups, incident response teams, etc.

A CES security roadmap is maintained, looking forward approximately three years. The roadmap is focused on needs and priorities that are common across CES. All IT professionals have a role in the security of IT data, systems, and services. The CES SOC does not maintain expertise in all IT disciplines and technologies. SOC employees are not a substitute for having IT professionals who are subject matter experts for an IT system or technology who are able to understand the security implications of implementation, configuration and management of that environment. The SOC roadmap does not account for all IT security risk reduction needs a campus has. Local priorities, implementation, and risk reduction can (and should occur) for areas where the CES security roadmap is not addressing or has not planned to address a risk that is important to an individual campus. Local IT security committees can assist to help create and implement a local campus security roadmap that complements the CES security roadmap (avoiding duplication of solutions or services), assess, measure, & resolve security risk, provide input to the CES security roadmap, etc. CES SOC staff are available to participate in local IT security committees.

Detailed documentation about the CES Information Security Program; current state of individual campus IT security hygiene; CES SOC pillars and focus; and CES security roadmap can be found at:

<https://byu.app.box.com/file/1758924390507> (limited distribution, authentication required)

Note: BYU-Pathway Worldwide, CES Seminaries & Institutes, and the Missionary Training Center on the BYU campus are outside the scope of the CES information security program and CES Security Operations Center. Those organizations receive security services from the church ICS organization.

"If you see something say something"

cessoc@byu.edu

cessoc@byuh.edu

cessoc@byui.edu

cessoc@ensign.edu

801-422-7788

The CES SOC is also available via local Teams channels