BYU

Church Educational System
Security Operations Center

Information Security Program

Contents

Last Updated: 16 Jan 2024

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

RELATED POLICIES: Appropriate Use of IT Resources Policy
Data Use, Privacy, and Security Policy

OVERVIEW

The Information Security Program describes Brigham Young University's general approach to protecting nonpublic institutional data in support of university policy. The primary objectives of the program are to 1) provide reasonable assurance nonpublic university information will be protected from unauthorized access, use, modification, or disclosure; and 2) comply with applicable state and federal laws and contractual agreements. The CES Security Operations Center (SOC) has primary responsibility for maintaining this Program. However, protecting nonpublic institutional data is a shared responsibility that includes all university units and personnel.

The information security program is overseen and implemented by the BYU Chief Information Security Officer:

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

Questions, comments, or concerns about the campus information security program can be sent directly to this individual.

The CES Security Operations Center (CESSOC) is run from the BYU campus to assess and reduce information security risk, test and monitor campus IT environments for cybersecurity threats, and respond to all information security incidents. Anyone (including students, faculty, and staff, as well as those not affiliated with the university) who believes that an information security incident has or may have occurred should notify the CESSOC at 801-422-7788. Questions, concerns, or issues can also be emailed to cessoc@byu.edu

RISK BASED PROGRAM MANAGEMENT

The operation and evolution of the Program is largely focused on addressing major campus information security risks, based on regular and ongoing assessment activities. These assessments are performed by both internal and external resources. Major risk areas currently identified include, but are not limited to the following:

- Vulnerabilities and Misconfigurations
- End of Life systems
- Phishing and Account Compromise
- Malware and Ransomware
- Undocumented or Non-assessed third party service providers with access to nonpublic institutional data

The CES Security Operations Center (CESSOC) actively works to reduce these risks, monitors systems for threats, and strives to respond to those threats in a timely manner.

USER AWARENESS AND IT CONTROLS

Employee Training and Awareness

Information security training and educational resources are provided to all employees and students as outlined below. New and refresher training is developed and delivered as needed or requested, based on new or ongoing risk or changes to the environment.

Information Security Training
Training modules that include the topics of basic security training, phishing, and password management are published in the university training systems. Central HR ensures that all new employees participate in the training as a part of the onboarding process. They also ensure that all employees take the security training as a refresher annually.

Developer Training
Developers and other IT professionals complete secure development training, aligned to the development framework they work in.

Phishing Simulation & Assessment
Phishing simulation exercises are conducted for employees to assess knowledge of phishing tactics and raise awareness among the campus community. Results of these exercises are used to target additional training and coaching efforts for campus units.

Awareness & Outreach Efforts
The CESSOC maintains a set of websites and webpages that include videos, articles, infographics, and other resources for security awareness. Awareness material promoting cybersecurity topics are regularly distributed through digital and print channels throughout the campus. Critical and timely information is shared in partnership with university communications through the employee newsletter.

Physical Security

Critical IT systems are to be physically secured in rooms that allow access only to authorized users. Visitors, contractors, and vendor service personnel are required to register and be escorted by authorized university personnel when accessing these systems.

Paper documents with nonpublic institutional data are to be kept in file cabinets, rooms or vaults that are locked each night. Only authorized employees are provided with access. Paper documents that contain nonpublic institutional data are to be shredded at time of disposal.

Security controls for campus IT resources

All IT resources are to meet the campus IT standards laid out at https://itstandards.byu.edu as per the university's Appropriate Use of Information Technology Resources Policy. The campus IT Standards are chosen to address, both directly and indirectly, the major campus information security risks described above. As new risks are identified and measured, the campus IT Standards are adjusted to provide appropriate and achievable controls for those risks.

Some university systems are subject to additional controls laid out by appropriate laws or regulations. These systems should first meet the campus IT standards requirements then follow any other requirements associated with the relevant law or regulation. Examples include:

- PCI scoped systems, which are currently following PCI-DSS 3.2.1 and working towards PCI-DSS 4.0 compliance with a target date of March of 2025.
- GLBA scoped systems, which are to meet the safeguards identified in 16 C.F.R. 314.4(c) (1)through(8) of that law.

Units with systems requiring additional security controls should consult with the information security risk managers in the CESSOC, who can assist them in developing a plan that allows them to implement further controls that align with the NIST Cyber Security Framework.

Monitoring & Prevention Mechanisms

The CESSOC monitors and protects campus endpoints and other IT assets for the presence of cybersecurity threats. These IT assets are protected with robust host-based security applications. Alert data is raised to the CESSOC to be reviewed and investigated.

The campus network is monitored both internally and at the campus border. Multiple systems are used to monitor and protect the campus network. These systems raise alerts that are also investigated by the CESSOC. Locations that are exceptions to this type of monitoring include the guest WiFi network at Lavell Edwards Stadium and the on campus housing network.

Assessment & Testing of Systems, Controls, and Protections

The CESSOC assesses system vulnerabilities and security on an ongoing basis. Host-based agents installed on each system monitor operating system and application version and patch levels and report any related vulnerabilities to the central CESSOC repository. Any system vulnerabilities are presented to system managers for remediation by priority of criticality.

The CESSOC penetration testing team proactively assesses system security for critical university systems, provides a detailed report to the corresponding system owner or management team, and consults where necessary with issue remediation.

The CESSOC information security risk management team assists campus IT personnel in their efforts to assess the current state of risks associated with their systems. The campus IT standards are used as a starting point for this assessment activity. The overall goal of this effort is to reduce IT risk for these systems, their data, and the campus as a whole.

Selection of Appropriate Service Providers
In choosing a service provider that will maintain or regularly access nonpublic institutional data, a review should be conducted to assess a service provider's ability to safeguard nonpublic institutional data according to university information security standards. This assessment is provided by the CESSOC following the process outlined in the Vendor Security Risk Assessment Process (https://infosec.byu.edu/vendorsecurityriskassessment) document. The Office of the General Council uses the results of this assessment in the determination of whether the associated contract needs to have the university Data Privacy and Security Addendum attached. (See the Legal Documents Policy.)

INFORMATION SECURITY INCIDENT RESPONSE PLAN

An incident response plan is maintained that outlines CES-wide procedures related to a major information security event. While each information security incident has unique aspects, this plan gives the incident response team overall guidelines for its responsibilities and actions.

The incident response plan allows the university to handle information security incidents in a way that provides several benefits:

- Avoiding or minimizing damage to individuals whose data has been compromised
- Helping the university community understand the process involved
- Minimizing the impact of the incident on the confidentiality, integrity, and availability of university systems and data
- Meeting legal requirements
- Protecting the reputation of the university

The incident response plan can be found at https://infosec.byu.edu/major-information-security-incident-response-plan.

ADJUSTMENTS TO THE INFORMATION SECURITY PROGRAM

This plan is subject to periodic review and adjustment as needed to reflect any changes in technology, emergent risk, the sensitivity of the information and internal or external threats to campus information security. The Chief Information Security Officer, in consultation with the Office of General Counsel and the Information Security and Privacy Committee (ISPC), will annually review the Information Security Program and recommend updates and revisions.

As campus units mature and existing risks are addressed, security program framework development should strive to align with NIST CSF standards, while maintaining their focus on ongoing risks to the people, systems, and data of the university.

Changes related to the acquisition of information security hardware or software tools are risk based and executed through the campus resource planning process. Every effort is made to ensure that the needs of the information security program can be met in this planning process.

RELATED INFORMATION

- infosec.byu.edu (Website of university information security processes and procedures)
- itstandards.byu.edu (IT Standards for all University IT resources)
- cessecurity.org (Security awareness training & materials)