BYU HAWAII

Church Educational System
Security Operations Center

GLBA Safeguards Element 3

Last Updated: 5 August 2025

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

OVERVIEW

This document describes in basic terms how the University is meeting the controls identified in Element 3 of the GLBA Safeguards identified in 16 C.F.R. 314(c) (3). This document is not intended to serve as a technical deep dive into the solutions or controls employed but serves as a description of how BYU-Hawaii operates to meet these controls.

AUTHENTICATION & ACCESS CONTROLS IN PLACE WITH PERIODIC REVIEW

Administrative access to university systems is granted by job function only. This access is automatically granted for some systems, based on job position, as hiring is completed. Administrative access to those university systems is automatically revoked when an individual's employment ends or when the employee's job function changes in a way that no longer justifies the need for the particular access. For systems not participating in the automated access, a Team Dynamics ticket is created with a four step approval process to grant the access.

See https://byuh.teamdynamix.com/TDClient/1902/Portal/KB/ArticleDet?ID=14140 for the terminated employee access review procedure.

DOCUMENT DATA, SYSTEMS, FACILITIES, & PERSONNEL

An IT inventory is maintained by OIT EIS that lists the business criticality, data classification level, hosting location, technical contact, and business contact for all University IT systems. See https://byuh.box.com/s/3c81q21f6sz5jqy1b2z4i2os9kqs140k for more details.

PROTECT BY ENCRYPTION ALL CUSTOMER INFORMATION

All application traffic between systems and the end user is to be encrypted via HTTPS. Plaintext HTTP interfaces are to be disabled or redirected to the HTTPS protocol. Direct administrative access to systems is performed via the campus provided VPN connection.

ADOPT SECURE DEVELOPMENT PRACTICES FOR IN HOUSE DEVELOPED APPLICATIONS

BYU-Hawaii has very little remaining in house developed applications, preferring a buy over build methodology for a number of years. All in house developers have had secure developer training performed through the HackEDU program provided by the CES Security Operations Center. Newly hired developers are to take the secure development training within the first month of their employment.

IMPLEMENT MULTIFACTOR AUTHENTICATION

Multifactor Authentication is a requirement for all campus systems that perform authentication activities as per the campus IT

standards defied at https://byuh-itstandards.prod.brigham-young.psdops.com/

The approved tool for multifactor authentication is Okta Verify, which is fully integrated to the campus Okta and EntrataAD authentication solutions.

IMPLEMENT A TWO YEAR DATA RETENTION POLICY & DISPOSAL PROCEDURE (POST USE)

All University systems should follow the University records retention policies. (See https://policies.byuh.edu/university-records-retention) University data retention policies vary between data domains, following the guidelines in the University's General Retention Schedule, found at https://oit.byuh.edu/https:/brightspotcdn.byu.edu/40/49/6a14e9304d24bfb9b1ea61d7c4d3/byuh-grs-01-2020.pdf. For GLBA systems, the post use data retention policy is set at two years.

FOLLOW CHANGE MANAGEMENT PROCEDURES

All changes to IT systems must follow the change management procedures identified at https://byuh.teamdynamix.com/TDClient/1902/Portal/KB/ArticleDet?ID=71614. Any changes released outside the change management process are reviewed and scrutinized by the IT management team.

MONITOR & LOG ACTIVITY OF AUTHORIZED USERS, DETECT UNAUTHORIZED ACCESS OR USE

University authentication and authorization systems should be configured to log all user activity to the campus LogScale environment. The CES Security Operations Center owns the responsibility for monitoring the activity of authorized users as well as the detection and response processes for unauthorized activity.