Student Financial Aid Information Risk Assessment

Overview

Section 314.4 of the Gramm-Leach-Bliley Act (GLBA) requires higher-education institutions to develop, implement, and maintain an Information Security Program to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of student financial aid information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. At a minimum, risk assessment documentation should consider risks related to a lack of employee training and management; information systems, including network and software design, information processing, storage, transmission and disposal; detecting, preventing and responding to attacks, intrusions, or other systems failures.

In general, to mitigate the risks associated with the areas above, we have taken the following steps.

- Risk assessment processes are conducted prior to implementation of major changes or technology and on an ongoing basis to identify and mitigate reasonably foreseeable threats.
- Employees sign acceptable use policies and receive training upon hire and annually thereafter to acknowledge and understand their responsibilities related to technology and protection of student information data.
- Controls and procedures have been implemented protect student information from implementation to disposal.
- Formal incident response processes and procedures have been implemented to proactively identify and investigate potential incidents, escalate those incidents to appropriate staff, and ensure timely remediation.
- Periodic testing of controls is conducted through a combination of internal and external review (ex: vulnerability scanning, penetration testing, general controls reviews, audit log monitoring, etc.),

General Threats

The following general technology risks exist to student information systems and student information data. General controls have been implemented to mitigate these risks, and Management will continue to expand risk assessment processes to further detail how these risks are mitigated.

- Natural disasters, pandemics, or man-made disasters
- Power or equipment failures
- Physical theft of data or break-ins
- External electronic intrusion and malware
- Employee or vendor fraud, error, or failure
- Constituent-initiated issues
- Social engineering and phishing
- Civil unrest

Application Threats

In addition to general threats, specific threats exist to each relevant application. Available controls for each system differ; therefore, the risks have been assessed on an application level and are detailed below.

Asset or Application	Purpose	Data Classification	Vulnerability	Likelihood	Impact	Risk Rating	Mitigating Controls	Residual Risk
National Student Loan Data System (NSLDS)	Compliance Vendor	Confidential	Unauthorized electronic data access by hacker, constituent, or other outsider or physical theft of server and data storage	M	H	H	• Data is uploaded to a secure vendor portal. • Limited number of users with access to vendor site. • Complex authentication controls are enforced by the system ○ Minimum of 8 characters with complexity enabled (alphanumeric with special character) ○ 5 invalid login attempts and then account is locked for 15 minutes ○ 15 invalid login attempts and then the account is locked until unlocked by an administrator	L
			Data corruption or loss	L	L	L	• Data is maintained by Department of Education after import.	L
			Vendor breach	L	H	M	• DoE has appropriate security controls, redundancy and breach notification procedures • The vendor was vetted prior to contract initiation.	L
			Unavailability	L	L	L	• Temporary unavailability of data, such as from an internet outage, does not materially affect operations. • Vendor maintains data backups and disaster recovery plans.	L