AMERICAN SAMOA COMMUNITY COLLEGE

GRAM-LEACH-BLILEY ACT (GLBA) RISK ASSESSMENT
Completed: 9/26/24

A. Identifying and Classifying Data

Nonpublic personal information (NPI) is "personally identifiable financial information that an institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available (Federal Trade Commission FTC, 2023, p4).

According to FTC (2023, pp4-5), "NPI is:

- any information an individual gives you to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application);
- any information you get about an individual from a transaction involving your financial product(s) or service(s) (for example, the fact that an individual is your consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or
- any information you get about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report)."

For ASCC risk assessments, NPI or Protected data can be one of the following Data Types:

1) **Provided Data**: Data provided by student to ASCC (Full Name, Social Security Number, Date of Birth, Address, Identification, Placement / SAT Scores, Personal Email Address, Phone Number)
2) **Institution Data**: Data created by ASCC for student as part of its services (Account Balance, Account Details, Check Amounts, Course Roster, Financial Aid Award Amounts, Grades, Login Credentials, Student ID, Transcript data, Student Email)
3) **Other:** Data otherwise obtained by ASCC about student

Data that is collected, stored, processed and shared by ASCC is categorized into these data types: Provided, Institution, and Other.

In reviewing processes and data definitions for this Risk Assessment, a change was made to state that all data collected by ASCC is restricted. Access to NPI or Protected Data is provided based on whether user needs this access. In the previous Risk Assessment, data was categorized as:

Private: Accessible to all Colleague System Users
Restricted: Accessible ONLY to a set number of users from different Divisions
Exclusive: Accessible to MIS ONLY

All NPI data is classified as Restricted. No NPI data is accessible to all Colleague users, and no NPI data is exclusively accessible to MIS only. Other changes were made in order to clarify the

list of protected data. Account Details was replaced by Account Number and Account Transactions. Course Roster, Transcript Data (Course History) and Transcript data (Grade History) were deleted and replaced with Transcript Data. Grades remains in the list because Grades are present in different areas apart from the Transcript Data. Financial Aid Expected Family Contribution (EFC). This was confirmed by Financial Aid Officer as being data that is available on the Colleague system.

The following provides a list of data types and whether it was provided by the student or the institution. This list is sorted by Data Type.

No.	NPI (Protected Data)	Data Type
1	Full Name (First, Middle, Last)	Provided
2	Date of Birth	Provided
3	Identification Data (Drivers License, Passport, etc.)	Provided
4	Social Security Number	Provided
5	Mailing Address	Provided
6	Phone Number	Provided
7	Personal Email Address	Provided
8	SAT / ACT Score	Provided
9	Account Number	Institution
10	Account Balance	Institution
11	Account Transactions	Institution
12	Refund Check Data	Institution
13	Financial Aid Award Data	Institution
14	Placement Test Scores	Institution
15	Transcript Data	Institution
16	Grades	Institution
17	Student ID	Institution
18	Login (Username and Password)	Institution
19	Financial Aid household data	Other (FAFSA)
20	Financial Aid Expected Family Contribution	Other (FAFSA)

B. ASCC Asset Inventory / Auditable Unit

All ASCC assets are listed as those that collect, store, process and/or share NPI for students are identified and each of these assets become an auditable unit for which threats are identified. Each Asset is mapped to the which NPI or Protected Data and data type that it collects, stores, processes, and/or shares. Auditable units have been updated to match the updated NPI Data and data types. No significant changes were made to identified assets since previous Risk Assessment.

Collect: Takes input or data entry from user
Store: Saves input to Storage (storage can be physical hard drive, network drive, or cloud)
Process: Takes input and turns it into a different set of output that is stored or returned to user
Share: Provides information to user (report export, screen display, print out, etc.)\

NO.	ASSET / AUDITABLE UNIT	DATA TYPE	DATA	COLLECT, STORE, PROCESS, OR SHARE	HOSTED BY ASCC ON-SITE	HOSTED BY VENDOR OFF-SITE
INFORMATION SYSTEMS						
1	Ellucian Saas for Colleague	Provided, Institution, Other	All data	Collect, Process, Store, Share		X
2	Self Service Saas for Colleague	Provided, Institution, Other	All data	Process, Share		X
3	Argos Reporting for Colleague	Provided, Institution, Other	All data	Process, Share		X
4	Google Workspace amsamoa.edu Email and Shared Drive	Provided, Institution	Full Name, Student ID, Login, Personal Email Address	Collect, Store, Share		X
5	Moodle Course Management System	Institution, Provided	Full Name, Login (username)	Collect, Store, Share		X

6	External Internet	Provided, Institution, Other	All data	Share		X
7	Firewall	Provided, Institution, Other	All data	Share	X	
8	Student Domain Controller / AD Server	Provided, Institution	Full Name, Login, Student ID, Personal Email	Collect, Store, Share	X	
9	Network Controller Server	Provided, Institution, Other	All data	Share	X	
10	Network Switches	Provided, Institution, Other	All data	Share	X	
11	Shared Folder Storage	Provided, Institution, Other	All data	Collect, Store, Share	X	
12	Systems Backup Storage	Provided, Institution, Other	All data	Store, Share	X	
13	Records Computers (2)	Provided, Institution	Full Name, Student ID, Transcript Data, Grades	Store	X	
14	Finance Computers (2)	Provided, Institution, Other	Full Name, Account Balance, Account Transactions, Refund Check Data, Student ID	Store	X	
PHYSICAL SYSTEMS						
15	Admissions Officer Files	Provided, Institution	Full Name, Date of Birth, Identification Data, Social Security Number, Mailing Address, Phone Number, Personal Email Address, SAT / ACT Score, Placement Test Scores (Application Data that is moved to Records File Archive when Late Admissions / Late Registration period is complete)	Store	X	

16	Records Division File Archive	Provided, Institution	Full Name, Date of Birth, Identification Data, Social Security Number, Mailing Address, Phone Number, Personal Email Address, SAT / ACT Score, Placement Test Scores, Transcript Data, Grades, Student ID	Store	X	
17	Finance Division File Archive	Provided, Institution	Full Name, Mailing Address, Phone Number, Account Number, Account Balance, Account Transactions, Refund Check Data, Student ID	Store	X	
18	Financial Aid Division File Archive	Provided, Institution, Other	Full Name, Date of Birth, Social Security Number, Mailing Address, Phone Number, Personal Email Address, Financial Aid Award Data, Student ID, Financial Aid household data, Financial Aid Expected Family Contribution	Store	X	

C. Identifying Threats / Risks

For each Auditable Unit, a list of threats is generated. The list of threats is created based on threats that have previously occurred on campus, in American Samoa, and those found through research and from monthly Cybersecurity newsletters, such as Center for Internet Security (2023) newsletter. No new threats were identified nor added this year. The current list was inclusive of those noted from threats and training presented this year.

A Third Party Risk Assessment will be used to assess risks for assets that are hosted off-site by an ASCC Vendor. The following provides a list of threats and the respective assets or auditable units, hosted by ASCC on-site, that these threats could potentially affect. The numbers used in this table corresponds to the Asset Inventory provided above:

Item. No.	Threat	Asset(s) or Auditable Unit(s) Affected

1	Ransomeware, Malware, Virus altering and/or destroying data	8,11,12,13,14
2	Hardware Failure destroying data	7 to 14
3	Software Failure destroying data	7 to 14
4	Power Failure corrupting software and/or hardware altering or destroying data	7 to 14
5	Power Failure resulting in no access to critical systems	7 to 14
6	External Internet Failure resulting in no access to critical system	7 to 14
7	Unauthorized physical access resuting in intentional or unintentional disclosure, misuse, alteration or destruction of data	7 to 18
8	Unauthorized System Access resulting in the intentional or unintentional disclosure, misuse, alteration or destruction of data	7 to 14
9	Phising Email or Smishing (SMS Phishing) results in installation of malware, ransomware, or compromise	8,11,12,13,14
10	Social Engineering, or Vishing (Voice Phishing) results in installation of malware, ransomware, or compromise	8,11,12,13,14

Using the Risk Matrix below, each threat is evaluated for how likely it is and the severity of the compromise. This identified the level of risk, and the Auditable Units were sorted by order of highest risk.

		Likelihood			
		Very Likely	Likely	Unlikely	Highly Unlikely
Severity	High	High	High	High	Medium
	Medium	High	High	Medium	Medium
	Low	High	Medium	Medium	Low
	Insignificant	Medium	Medium	Low	Low

Attached is a Risk Assessment spreadsheet including all data used for the risk assessment performed and this narrative. It includes the following tabs:

- Data Types
- Assets
- Threats
- Risks and Controls – ASCC Hosted
- Risks and Controls – Vendor Hosted
- Interviews
- Findings and CAP (Corrective Action Plan)
- Previous Findings and CAP

The Risks and Controls tab holds the details of the Risk Assessment performed, the column headings for this assessment are:

Threat	Auditable Unit at Risk	Likelihood	Severity	Risk Level	Responsible	Control / Prevention	Detection	Response	Policy / Reference	Recommendation	Finding / Action Plan #s	Findings	Corrective Action Plan (CAP)	Current Control

Employee training and management.

After a review of the Governance Policy Manual and Divisional Standard Operating Procedures (SOPs) for Divisions that handle and have access to NPI, interviews were for performed with Acting Registrar, Financial Aid Officer, Acting Admissions Officer, Acting Finance Officer, and HR Officer. This year's review of the processes for HR confirmed that HR handles NPI through the Summer Youth Employment Program (SYEP)_where students are employed by ASCC. HR was included in the list of offices interviewed this year. The following presents the questions and responses from these interviews:

	Questions	Acting Registrar / Records Officer	Financial Aid Officer	Acting / Admissions Officer	Acting Finance Officer	HR Officer
1	Does your office perform training or orientation for employees on the policies on privacy and confidentiality of student records, or any ASCC records?	Yes. All new employees are provided orientation on FERPA and it is included on their job description; Student hires sign an FERPA Confidential Agreement before working in the Records Office. During Student Orientation, Registrar presents in student rights under FERPA.	Yes, all new employees are provided orientation on the policies regarding the privacy and confidentiality of student records. The orientation ensures that all staff members are aware of their responsibilities and the legal implications of mishandling private student information. The orientation covers; FERPA (Family Educational Rights and Privacy Act) regulations, which protect the privacy of student education records. Data security protocols to ensure that sensitive information, such as Social Security numbers and financial details, is handled properly. Confidentiality requirements for sharing and accessing student data, ensuring employees understand when and how student records can be disclosed.	Yes. All new employees are provided orientation on FERPA. Student hires sign a FERPA Confidentiality Agreement before working in the Admissions Office. This year, new Staff have signed an Admission Confidentiality Agreement that covers FERPA regulations with regards to all student records and office related materials. This documentation is filed with the HRO office. Admissions student workers both Pell and Non Pell agreements are filed in the Admissions office.	Yes. Staff is trained on confidentiality of all data. Currently there is no FERPA, but will implement a process to train on FERPA and student data confidentiality	Yes. HR Officer performs annual training for the institution on Policies, including privacy and security. All new employees go through an orientation that includes review of job description, privacy and security policies. HR staff has monthly meetings where privacy policies are reinforced.

2	Do you save employee or student record information on your computer?	Yes. Two staff members save transcripts to computers before saving to shared folder used securely release transcript. These files are cleaned out weekly. Rosters and Grade sheets are replaced with faculty access to Self-Service (Colleague)	No, storing employee or student records directly on individual computers is not recommended in the financial aid offices due to security risks. Student and employee records, are stored in a secured share folder with controlled access. This system is in place to comply with FERPA.	No. All application attachments sent electronically are printed for the student file, then immediately deleted. No student information is saved in the computer.	Yes. Two employees save financial aid batching data on computer.	Yes. The only student data that ASCC HR handles is for Summer Youth Employment Program (SYEP) that is coordinated by the American Samoa Government HR Department, where students are able to be employed part-time by ASCC. This information is provided to ASCC on hard copies, they are scanned and saved in a shared drive and deleted from the computer.
3	Do you have a disposal policy, written or unwritten?	No. Records Office does not discard records because they have not yet been digitized, and Records plans to digitize records, then implement a disposal plan. Records Office does not have a disposal policy but adheres to the institution's disposal policy regarding equipment. Records does not dispose of student records but shred documents with any student information.	Yes, the financial aid office has a written disposal policy in the SOP. Student and financial records are retained 3-5 years before disposal. The financial aid office burns them at a designated location on campus. The financial aid officer is responsible for overseeing and executing the disposal of sensitive materials. This protects the privacy and confidentiality of personal information	Admissions Office does not keep student records. All application attachments electronically submitted are printed then immediately deleted. Admissions only keeps application files (locked in Admissions Officer's Office) until the end of Late Admission and Late Registration Period. Then files are moved to the Records Office File Archive.	Yes, there is a Disposal Process. Finance follows the written Procurement SOP to dispose of records more than 7 years old.	Yes, there is a Disposal Process. HR dispose of records more than 7 years old.

4	Do you train your employees on data confidentiality?	Yes.	Yes, the financial aid office has been trained on FERPA, data security protocols and confidentiality practices. The Information Officer provided training on cybersecurity to ensure staff are equipped to handle data securely.	Yes.	Yes.	Yes.
5	Have there been any data breach in your office since the last Risk Assessment?	No.	No. There has not been any reported data breaches in the financial aid office since the last risk assessment. Staff training and compliance with FERPA help ensure data remains secure.	No.	No.	No.

Since the last Risk Assessment, a Compliance Officer has been hired for ASCC. From a review of the answers to Risk Assessment interviews, the following recommendations are made:

1) Assign the responsibility of providing annual training on FERPA regulations and protection of nonpublic personal information of students to the new Compliance Officer
2) Adopt the process of deleting all NPI from computer hard drive and only to be saved in locations such as Shared Folders provided by ASCC or shared folders in Google Drive.
3) Create standard non-disclosure / FERPA agreement form for all who handle NPI to sign and place with HR file
4) Schedule annual training for all employees regarding GLBA and Privacy Policies
5) Include GLBA, FERPA requirements for privacy of NPI in Position Descriptions of all employees who handle NPI
6) At next review of Policy Governance Manual, review policies noted in Data Information Security Program (DISP) Plan (also included below) to add privacy and confidentiality requirements

The following policies in the Governance Manual discuss data privacy, confidentiality, and enforcement of these policies:

- Policy 3012.1 Archives
- Policy 3022 Official Correspondence
- Policy 3022.1 Correspondence Detail

- Policy 3023 Standard Filing System
- Policy 3024 Distribution of Keys
- Policy 3025 Intellectual Property
- Policy 4007 New Employee Orientation
- Policy 4203 Employee Code of Conduct
- Policy 4205 Employee Privacy Rule
- Policy 4205.1 Collecting and Retaining Personal Information
- Policy 4205.3 Disclosure of Employee Information
- Policy 4505.4 File Retention
- Policy 4301 Disciplinary Actions
- Policy 4301.1 Disciplinary Action, Suspension and Dismissal
- Policy 4306 Training Programs
- Policy 4411 Acceptable and Safe Use of College Equipment, Property and Services
- Policy 5003 Family Educational Rights Privacy Act (FERPA)
- Policy 5105 Faculty Use for Copyrighted Materials
- Policy 6200 Campus Safety
- Policy 6101 Use of College Property / Removal of College Property from College Premises
- Policy 6210 Campus Security
- Policy 7006 Inventories of Materials and Equipment
- Policy 7006.1 Sale or Disposal of Property or Equipment
- Policy 9000 Information Technology Purpose
- Policy 9001 Rights and Responsibilities
- Policy 9002 Confidentiality
- Policy 9003 Existing Legal Context
- Policy 9004 Copyright
- Policy 9009 User’s Credentials
- Policy 9010 Transmission of Personal Information
- Policy 9011 Decoding
- Policy 9012 Disruptive Use

- Policy 9013 Copyright Software
- Policy 9014 Systems Misuse
- Policy 9015 General Prohibition
- Policy 9017 Privacy
- Policy 9018 Electronic Mail
- Policy 9019 Internet Access
- Policy 9020 Social Networking
- Policy 9021 Harassment
- Policy 9022 Intellectual Property
- Policy 9024 Security
- Policy 9025 Violations
- Policy 9026 Enforcement

Since the previous Risk Assessment, one training has been completed to share the importance of Security NPI and Cybersecurity.

Information Systems and Information Processing and Disposal.

The attached Risk Assessment spreadsheet details the information system assets that collect, store, process and share nonpublic personal information for students. Risk levels range from Medium to High. Because of this, ASCC should ensure that information systems are properly secured while it is active in the ASCC inventory, and then properly disposed and sanitized according to the ASCC Policy Governance Manual, SOPs and Systems Development Life Cycle (SDLC) Plan.

Detecting, Preventing and Responding to Attacks.

The attached Risk Assessment spreadsheet details risk Prevention, Detection and Response. The Management Information Systems (MIS) Division uses a work order tracking system called OS Ticket to enter in all requests or technology issues reported to MIS. Risk documented would create work orders with Priority Levels ranging from High to Emergency. This is because of the urgency to resolve issues with systems that hand nonpublic personal information of students.

D. Risks and Controls

The attached Risk Assessment spreadsheet includes two tabs: a) Risks and Controls-ASCC Hosted, which contains Risks and Controls for information systems that are hosted on premises by ASCC, and b) Risks and Controls-Vendor Hosted, which contains Risks and Controls for information systems that are hosted off campus by a third-party vendor. For the items where the control needed improvement, Recommendations were added. If an item had a finding, that was listed in the Findings column. Some risks had the same finding. A Findings list (provided in the next section) was created to number each type of finding. Each finding also correlates to a Corrective Action Plan (CAP) and it includes an estimated time of completion in the narrative. This list is then used to standardize each finding and CAP. If the control was enough to mitigate the risk, then an entry of "None" is entered for the Findings and CAP.

E. Findings and CAP

This list was created by combining the types of findings that were the same for different risks. Each Finding is assigned a CAP with an estimated time of completion. The Risk Assessment Spreadsheet was updated to show the Finding and CAP for each Risk Item. ASCC expects to have the findings addressed within the next Fiscal Year and will report updates on the next Risk Assessment to be performed by 9/30/2024.

No.	Threat	Finding	Corrective Action Plan (CAP) Items	Due Date	Current Control
1	#4 Power Failure corrupting software and/or hardware altering or destroying data #5 Power Failure resulting in no access to critical systems	1) Generator for main campus automatic switch is not working, so it has to manually be switched on.	1) Complete work by Electrical consultant to troubleshoot Automatic Transfer Switch. 2) Replace main campus Generator based on updated plan. Completed by September 30, 2025.	9/30/2025	1) Smart UPS units are installed for critical servers so that they are automatically shut down when there is a power outage. Generatory is manually turned on to restore stystems until power is restored.

2	#6 External Internet Failure resulting in no access to critical system	1) Users of Colleague SAAS are not able to log in when the backup ISP is activated if the primary is unavailable	1) Work with Backup ISP and Ellucian to allow Authentication to work when ASCC on backup connection.	12/31/2024	1) MIS support contract with primary ISP is immediate, they are contracted to restore connectivity within 1-2 hours in order to restore this service.

F. Previous Findings and CAP

This tab was added in 2022-2023 to provide an update on previous findings and CAP status. It reflects the same information as the "Findings and CAP" but provides additional columns with dates and updates to the progress of the CAP for each finding. Since the previous Risk Assessment, all Corrective Action Plans (CAP) were completed except for Item No. 3. The Incident Response and SDLC Plans are marked as complete as this is a documented plan that supports the processes already undertaken. The final draft of the plans have been submitted for review and approval. CAP for item No. 3 is expected be completed in FY 2024-2025.

No.	Threat	Finding	Corrective Action Plan (CAP) Items	Due Date	Current Control	Status as of 9/26/2024
1	ALL Threats	There is a need to create Incident Response Plan to support incident reporting and response process already being used.	Create Incident Response Plan.	11/30/2023	Incident Reports are documented and submitted to executive leadership for major security issues, including all threats listed in Risk Assessment.	**9/25/2024** **Complete.** Incident Response Plan submitted for approval
2	#2 Hardware Failure destroys data #3 Software Failure destroying data	There is a need to create System Development Life Cycle (SDLC) Plan to support processes already being used.	Create a SLDC Plan	12/31/2023	MIS renewals hardware up to 2 years prior to hardware reaches 5 years of use to stay current. Hardware replacement is planned for FY2024-2025.	**9/25/2024** **Complete.** SDLC Plan submitted for approval

3	#4 Power Failure corrupting software and/or hardware altering or destroying data #5 Power Failure resulting in no access to critical systems	Generator for main campus automatic switch is not working, so it has to manually be switched on.	Replace main campus Generator. Completed by March 31, 2024.	3/31/2024	Smart UPS units are installed for critical servers so that they are automatically shut down when there is a power outage. Generator is manually turned on to restore stystems until power is restored.	**9/23/2024** In August, a local vendor was able to provide a quotation, and a specialist visited on 9/6/24 to review the current generator. Based on this, vendor was hired to troubleshoot issues with current generator automatica transfer switch. At the same time, plan for replacement of generator was updated. Replacement of generator will be completed by 2024-2025.
4	#6 External Internet Failure resulting in no access to critical system	Recommend to increase bandwidth of Secondary ISP connection to better handle the load on the Firewall	1) Increase bandwidth for Secondary ISP. Complete this by 11/30/2023.	11/30/2023	Configuration on Sonicwall is updated to allow only critical systems to connect to Secondary ISP so that access is available to Colleague and Moodle users from a connection off campus or through data.	**11/7/2023** **Complete.** Bluesky updated contract for 240Mbps signed and executed. MIS confirmed speetests.

5	#7 Unauthorized physical access resuting in intentional or unintentional disclosure, misuse, alteration or destruction of data	Recommend to move security camera once Financial Aid Office completes move	Move security camera once Financial Aid Archive is moved to new location	3/31/2024	Financial Aid archives are located in a locked roomw with restricted access. This is monitored by Financial Aid Officer.	**10/21/2023 Complete.** Financial Aid Camera Installed in current location
6	Does not meet requirement that the service provider have documented appropriate safeguards and controls (e.g. SOC2) to protect NPI for ASCC students, and that it must promptly report any security incidents that may affect ASCC Student NPI	Security information is not included in the contract nor documented online.	Request for this information to be available and included in ASTCA contract	10/31/2023	ASTCA is an Internet Service Provider, and risks are limited to packet sniffing and monitoring flow of data through lines. Data from critical systems is encrypted.	**10/12/2024 Complete.** ASTCA responded and sent their ISP Cybersecurity Policies
7	Does not meet requirement that the service provider have documented appropriate safeguards and controls (e.g. SOC2) to protect NPI for ASCC students, and that it must promptly report any security incidents that may affect ASCC Student NPI	Security information is not included in the contract nor documented online.	Request for this information to be available and included in Bluesky contract	10/31/2023	Bluesky is an Internet Service Provider, and risks are limited to packet sniffing and monitoring flow of data through lines. Data from critical systems is encrypted.	**10/4/2023 Complete.** Bluesky responded and sent their ISP Cybersecurity Policies

G. Review of Risk Assessment Process

The changes in each step of the process is stated throughout this document. Major recommendations from this Risk Assessment includes those to be assigned and include the new Compliance Officer.

Challenges to this process included multiple projects funded under grants that are on the final year for completion as well as new Financial Aid requirements that began for Aid Year 2024-2025 that required immediate attention. This caused the Risk Assessment originally planned to be performed in February, to be delayed and completed in September. After further review of the quarterly calendar, it is recommended that the next Risk Assessment be performed at the middle of the Fiscal Year, by the end of April 2025.

Monthly updates are noted in the spreadsheet tab marked “Previous Findings and CAP” to update the status of each CAP item. The Status updates from the previous Risk Assessment are also included in this Risk Assessment.

References

ASCC Division of Student Services (DOSS) Standard Operating Procedures (SOP) Manual. (2020-2022). Retrieved September 1, 2022 from https://amsamoa.edu/00_NON-WEBSITE/Evidence_2021_SelfEvaluation_Report/Standard1B/1B-DOSS_SOPs.pdf

ASCC Human Resources SOP Manual. (2020-2021). Retrieved September 1, 2022 from https://amsamoa.edu/00_NON-WEBSITE/Evidence_2021_SelfEvaluation_Report/Standard3A/3A-HR-SOPs.pdf

ASCC Management Information Systems SOP Manual. (2020-2021). Retrieved September 1, 2022 from https://amsamoa.edu/00_NON-WEBSITE/Evidence_2021_SelfEvaluation_Report/Standard3C/3C-MIS_SOPs.pdf

Cloud Security at Ellucian. (2023). Ellucian. Retrieved August 20, 2023, from https://www.ellucian.com/security

Ellucian Commitment to Privacy. (2023, August 3). Ellucian. Privacy Notice. Retrieved August 20, 2023, from https://www.ellucian.com/privacy

Federal Trade Commission (2023). What information is covered? *How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act – A Guide for Small Business from the Federal Trade Commission.* Retreieved March 31, 2023 from https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf

Policy Governance Manual. (2020). American Samoa Community College. Retrieved September 1, 2022 from https://amsamoa.edu/00_NON-WEBSITE/Evidence_2021_SelfEvaluation_Report/Standard1A/1A-2020_ASCC_Policy_Governance_Manual.pdf

Talanei. (2023, August 22). $4 Million transfer under investigation. Retrieved 8/25/2023, from https://www.talanei.com/2023/08/22/4-million-transfer-under-investigation/