Data Privacy, Cyber Incident & Information Security Response Plan

Overview

In accordance with the U.S. Department of Education's implementing regulations at 34 C.F.R., the Standards for Safeguarding Customer Information at 16 C.F.R. Part 314 issued by the Federal Trade Commission (FTC), the Family Educational Rights and Privacy Act (FERPA), and the Gramm-Leach-Bliley Act (GLBA), P.L. 106-102, Detroit Extravagant Academy (DEA) maintains safeguards designed to protect sensitive and personally identifiable information.

Upon signing a Program Participation Agreement (PPA), institutions participating in Federal Student Aid (FSA) programs are required to comply with applicable information security requirements. Colleges participating in FSA programs are subject to information security requirements established by the FTC for financial institutions.

DEA is responsible for complying with limitations on the disclosure of personally identifiable information (PII) contained in students' education records under FERPA and applicable provisions of the GLBA.

The Financial Services Modernization Act of 1999 (Public Law 106-102, 113 Stat. 1338), also known as the Gramm-Leach-Bliley Act, regulates the protection, collection, and disclosure of consumers' nonpublic personal information or personally identifiable information (PII) by financial institutions.

As an institution covered under applicable information security requirements, DEA has developed, implemented, and maintains a comprehensive data and information security program. The program is designed to:

- Maintain a written incident response plan.
- Implement safeguards to control identified risks.
- Regularly monitor and test the effectiveness of safeguards.
- Train staff regarding information security.
- Monitor service providers.
- Keep the Information Security Program current and responsive to emerging risks.

DEA receives annual risk and technology assessments from Electronic Brain Solutions (EBS). These assessments include control analyses, risk analyses, recommended control measures, and threat and vulnerability assessments.

DEA has qualified staff members who oversee and implement this program and report annually to the appropriate boards regarding changes, deletions, additions, and recommendations.

Designated Qualified Employees & Responsible Personnel

- **Fatimah Reese – School Director**
- **Christopher Plummer – School Administrator**
- **Third-Party Contractual IT Company**

Plan Evaluation, Revision, and Training

The Data Privacy, Cyber Incident & Information Security Response Plan is maintained in the Title IV Manual in hard-copy format throughout the school and digitally on the school's website.

This plan is reviewed annually by school committees and employees.

Training regarding this plan is conducted annually with the personnel responsible for implementing the plan and the third-party contractor responsible for DEA's onsite and offsite information technology services.

Information Security Plan

This Information Security Plan ("Plan") describes safeguards implemented by DEA to protect covered data and information in accordance with the FTC's Safeguards Rule promulgated under the Gramm-Leach-Bliley Act (GLBA).

DEA utilizes updated firewall configurations, protection measures, and security software, including Huntress, Webroot, Canauri, RMM monitoring, and penetration-testing scans.

These safeguards are designed to:

- Ensure the security and confidentiality of covered data and information.
- Protect against anticipated threats or hazards to the security or integrity of covered information.
- Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to a customer.

Information Security Program

DEA has developed written policies and procedures to manage and control information and identify and assess risks that may threaten covered data and information maintained by the institution.

Directories have been created and controlled to allow data to be shared in centralized, controlled locations.

The program is reviewed and adjusted as necessary through ongoing discussions and annual meetings concerning technology with staff, board members, and IT contractors. These reviews allow DEA to consider changes in technology, the sensitivity of covered data and information, and internal and external threats to information security.

Risk Management & Compliance Assessment of Risks to Student/Customer Information

Risk assessments are conducted to identify, quantify, prioritize, and manage risks.

Controls applicable to each situation are implemented to help prevent violations of legal obligations, including statutory, regulatory, and contractual obligations. These controls are also assessed through Electronic Brain Solutions (EBS).

DEA recognizes that it is exposed to both internal and external risks, including, but not limited to, the following:

Unauthorized Access

To prevent unauthorized access to covered data and information, access is limited to authorized individuals with a legitimate need to access specific information.

DEA has implemented risk-management and compliance practices that include:

- Locking doors to restricted areas.
- Locking computer screens when devices are not in use.
- Preventing sensitive information from being left visible on unattended screens.
- Using strong computer passwords.
- Restricting data access to authorized individuals.

These measures are designed to reduce the likelihood that data or information will be compromised through unauthorized system access.

Interception of Data

The DEA Business Center is responsible for the setup and management of email systems through Microsoft.

Messages containing sensitive information sent through authorized Microsoft systems are protected using appropriate security measures. Employees are prohibited from using personal Gmail accounts to transmit PII.

Offsite data backups are encrypted both in transit and at rest.

Privacy Settings

Privacy settings on each device may be configured to limit the amount of personal data that is shared.

Data Backup

DEA utilizes Western Digital Backup along with cloud-based image backups to protect data and information offsite through encryption.

Backup and security systems are also used to assist in detecting and remediating:

- System errors.
- Data corruption.
- Unauthorized access to covered data and information.
- Unauthorized requests for covered data and information.
- Pretext calling.
- Unauthorized access to hard-copy files and reports.
- Unauthorized transfer of covered data and information through third parties.

DEA policy prohibits unauthorized individuals from accessing another person's PII.

Hard-copy files are maintained in locked, fireproof cabinets located within a secured records room.

Third parties are vetted and are not permitted to access protected data unless authorized and appropriately supervised by DEA personnel.

DEA recognizes that these risks do not represent a complete list of risks associated with protecting covered data and information and that new risks may arise regularly.

The DEA Information Security Program Coordinator, together with Electronic Brain Solutions, will monitor appropriate cybersecurity advisories and resources to identify emerging risks.

An annual third-party penetration test and remediation assessment is also conducted.

Current safeguards are implemented, monitored, and maintained by the DEA Information Security Program Coordinator and Electronic Brain Solutions.

Based on current risk assessments, these safeguards are intended to provide appropriate security and confidentiality for covered data and information maintained by the school and to reasonably protect against anticipated threats or hazards to the integrity of such information.

Personnel Security Policy and Procedure

References and/or background checks, as appropriate for the position, are conducted for new employees who will regularly work with covered data and information, financial information, or financial aid information.

DEA also maintains contractual agreements designed to protect client and customer information.

Training & Awareness Policy and Procedure

Employees are trained annually regarding this plan, including changes and revisions.

Employees are instructed regarding acceptable practices for handling client and student data and the secure use of applications and technology solutions.

During employee orientation, each new employee whose position involves protected information receives training regarding:

- The confidentiality of student hard-copy and digital records.
- User groups and access permissions.
- Student financial information.
- Other covered data and information.
- Proper use of computer systems.
- Password security.
- Procedures for preventing unauthorized disclosure.
- Proper disposal of documents containing covered data and information.

These training efforts are intended to minimize risk and safeguard covered data and information.

Refresher training is required annually.

Physical Security Plan/Policy

DEA has implemented physical security measures to prevent unauthorized parties from accessing sensitive data.

Access is limited to employees who have a legitimate business need to handle such information.

For example, financial aid applications, income and credit histories, accounts, balances, and transactional information are available only to DEA employees with an appropriate business need.

Each department responsible for maintaining covered data and information must take reasonable steps to protect the information from destruction, loss, or damage caused by environmental hazards such as fire, water damage, or technical failures.

The policy also provides procedures for permitting physical access to alternate authorized individuals when primary authorized personnel are unavailable.

Information Systems Network Security Plan/Policy

Access to covered data and information through DEA computer information systems is limited to employees and faculty members who have a legitimate business reason to access such information.

DEA maintains policies and procedures, including access-control lists for data stored on its servers, to complement physical and technical safeguards.

Social Security numbers are considered protected information under applicable requirements of both GLBA and FERPA.

Existing controls include:

- Access restricted to authorized individuals.
- Password-protected workstations.
- Electronic information encrypted and transmitted only by authorized individuals.
- Continuous monitoring and remediation of network and system vulnerabilities.
- Systems managed through a managed-services platform to ensure appropriate patching.
- Unauthorized third-party access is prohibited.

Logical Access

Processes are maintained to prevent unauthorized access to systems. Users are assigned permissions and groups based on their job functions.

Controls include:

- All users must have unique user IDs for Windows and applicable third-party software.
- Email systems require unique user IDs and passwords.
- User access rights must be adjusted as necessary to reflect employees' current job responsibilities.

Operations Management

Operational procedures are established to protect documents, computer media, removable media, disks, input/output data, and system documentation from unauthorized disclosure, modification, removal, or destruction.

These procedures include:

- Sensitive data must be handled only by authorized personnel.
- Equipment containing data that has been decommissioned or repaired must have data securely wiped in accordance with applicable standards before disposal or reuse.
- IT providers will conduct testing as necessary.
- Employees may utilize appropriate verification procedures to ensure data is entered correctly and is not unintentionally modified.
- Changes to equipment or software must be communicated to designated employees who are trained to use the modified systems appropriately.

Management of System Failures

The DEA Information Security Program Coordinator maintains procedures designed to detect actual or attempted attacks against DEA systems and procedures for responding to actual or attempted unauthorized access to covered data and information.

In the event of a system failure, the Program Coordinator and/or contracted IT company must first determine the cause of the failure.

If the failure is caused by corrupt files or hardware failure, the issue should be addressed and data restored from available backups.

If the failure is determined to be the result of a malicious third-party attack, affected machines should be disconnected from the network while remaining powered on when appropriate.

The cybersecurity insurance provider should be contacted for guidance regarding the appropriate response within the parameters of the applicable policy.

Oversight of Service Providers

Electronic Brain Solutions and DEA oversee applicable service providers in accordance with GLBA requirements.

DEA takes reasonable steps to select and retain service providers that maintain appropriate safeguards for covered data and information.

The Information Security Program requires applicable service providers to implement and maintain appropriate safeguards through contractual requirements.

Procedure for Reporting Security Breaches to Students and the Department

DEA recognizes that a breach involving student records or information may create significant regulatory and administrative concerns.

In accordance with applicable Department of Education requirements, actual or suspected breaches involving the security of student records and information must be reported to the appropriate Department of Education contact as required.

Reports should include, as applicable:

- Date of the suspected or known breach.
- Impact of the breach, including the approximate number of affected records.
- Method of the breach, such as hacking or accidental disclosure.
- Information Security Program point-of-contact email address and telephone number.

- Remediation status, including whether remediation is complete or in process.
- Next steps, as necessary.

Where appropriate and required, affected students should also be notified.

Procedures to Maintain Compliance with the GLBA Regarding Personally Identifiable Information (PII)

1. Secure Storage of Records Containing PII

All records containing PII must be stored and maintained in secure locations.

- Paper records and files are stored in locked, fireproof cabinets located in secured rooms that remain locked when unattended.
- The Director of Operations controls access to restricted records areas.
- Stored data are protected against destruction or damage from hazards such as fire and flooding through appropriate safeguards.
- Electronic customer information is stored on secure systems with access controlled by the Information Security Program Coordinator and Electronic Brain Solutions.
- Access to electronic information is password protected and unavailable to students unless specifically authorized.
- Staff computers are password protected.
- Students are prohibited from accessing staff computers.
- Student and employee PII must be maintained on appropriately secured systems.
- Student information is backed up regularly through Electronic Brain Solutions.
- Backups are maintained in secure locations as determined by the Director of Operations.
- Credit card information is processed through the institution’s authorized payment processor.

2. Electronic Transmission of Student and Employee PII

All electronic transmissions of student and employee PII must be appropriately secured.

- Social Security information, IRS information, and other sensitive financial data transmitted directly to DEA must use secure connections or other currently accepted security standards.
- Students are advised against transmitting sensitive information through unsecured email.
- DEA requires applicable inbound transmissions of PII from third parties to be encrypted or otherwise appropriately secured.

- Outbound transmissions of PII must be secured in a manner approved by the Information Security Program Coordinator.
- If PII must be transmitted through email, the information must be password protected, encrypted, or otherwise secured against compromise.
- The Information Security Program Coordinator and applicable third-party service providers review systems and applications to ensure appropriate levels of security.

3. Paper Transmission of Student and Employee Information

Paper transmissions containing student or employee information must be appropriately secured.

- PII delivered to authorized third parties must remain appropriately sealed and protected.
- Paper-based student and employee information must never be left unattended in unsecured areas.
- Paper records must be maintained in locked, fireproof cabinets within secured records areas when not in use.

4. Secure Disposal of PII

All PII must be disposed of securely.

- The Information Security Program Coordinator will supervise the disposal of records containing PII.
- Paper-based PII must be shredded or otherwise securely destroyed.
- Hard drives, magnetic media, and other electronic media containing PII must be securely erased and/or destroyed before disposal.
- Hardware must be appropriately recycled or disposed of after protected information has been removed.
- PII must be securely disposed of after all applicable retention requirements have been satisfied.

5. Inventory of Devices

The Information Security Program Coordinator maintains an inventory of school computers and applicable devices on or through which PII may be stored, accessed, or transmitted.

6. Oversight and Audit Procedures

The Information Security Program Coordinator develops and maintains appropriate oversight and audit procedures to detect improper disclosure, unauthorized access, or theft of student information.

Definitions

Customers

For purposes of the Gramm-Leach-Bliley Act and this program, “customers” include individuals to whom DEA provides applicable services.

Customer Information

For purposes of this Safeguarding Program, “customer information” means any record containing nonpublic, personally identifiable financial information regarding an DEA customer, whether the information is maintained on paper, electronically, or through another medium.

This security program does not create contractual agreements between a student and another entity or person.

Applicability

This program applies to all DEA departments with access to student loan data or other customer information, regardless of the purpose or frequency of use.

It applies to the gathering, storage, processing, transmission, and disposal of customer information.

The program also applies, as appropriate, to outside service providers, including loan servicing agents and collection agencies, to which student loan data may be transferred or that may collect such information on behalf of DEA.

Information Security Program Policies and Procedures

Through updated firewall configurations and protection and security software, including Huntress, Webroot, Canauri, RMM monitoring, and penetration-testing scans, DEA implements, maintains, and enforces safeguards designed to detect, prevent, and respond to attacks, intrusions, and other system failures.

DEA also utilizes SMART educational management software as part of its school management infrastructure.

Authorized school administrators must use unique login credentials and passwords to access protected systems.

Information Security Program Coordinator

The DEA Information Security Program Coordinator is **Fatimah Reese, School Director**.

The Coordinator is responsible for ensuring DEA maintains adequate procedures to address compromises of the institution’s information safeguards.

Procedures include appropriate responses to specific types of incidents, including:

- Hacking.

- General security failures.
- Denial of access to databases.
- Denial of access to computer systems.
- Other cybersecurity incidents.

DEA utilizes a combination of hardware and software solutions to protect its infrastructure.

The Information Security Program Coordinator and appropriate IT personnel are responsible for:

1. Maintaining a working knowledge of appropriate technology for protecting student PII.
2. Coordinating appropriate security training throughout the year.
3. Ensuring DEA installs necessary updates to address software vulnerabilities and maintaining communication with DEA's IT provider.
4. Ensuring applicable updates and patches are installed and monitored for issues or failures.
5. Ensuring DEA uses appropriately maintained antivirus and endpoint detection and response (EDR) software.
6. Ensuring DEA maintains current firewall protections.
7. Managing DEA's information security tools and communicating relevant information regarding security risks and breaches to employees.
8. Implementing established procedures in the event of computer or technological failures to preserve the security, confidentiality, and integrity of student PII.
9. Ensuring access to student information is granted only to legitimate and authorized users.
10. Promptly notifying students when required if their PII has been compromised.

DEA maintains procedures for contacting individuals whose personally identifiable information is affected by a data breach in accordance with applicable notification laws and regulations.

DEA may also utilize monitoring and response services available through Electronic Brain Solutions and applicable insurance coverage.

Cyber Incident Response Plan/Policy

In the event of a cyber incident, including ransomware, a data breach, or a successful phishing attack, qualified coordinators and/or the IT provider must take appropriate response actions, including:

1. Disconnect the affected computer from the network while keeping the system powered on when appropriate. This may be accomplished remotely through security software or may require physical disconnection.
2. Notify the qualified individual and Electronic Brain Solutions if they have not already been notified.
3. Contact the applicable cyber liability insurance provider for instructions regarding how to proceed.

4. Follow the insurance provider's instructions regarding next steps, including whether a third-party investigator or incident response unit is required.

Physical Incident Policy

In the event of a physical disaster, such as a fire or flood, the following actions must be taken:

1. The Coordinator must obtain authorized access to the school, when safe and permitted, to assess damage to physical storage and technology.
2. The applicable insurance provider must be notified following the initial assessment.
3. Qualified coordinators and Electronic Brain Solutions will conduct an onsite evaluation of affected IT equipment.
4. Following the assessment, necessary steps will be taken to restore backup files, replace or restore servers, and return essential business applications to operation as soon as reasonably possible.
5. Physical media will be evaluated for damage and potential restoration.
6. If physical IT equipment is unusable, an appropriate temporary or cloud-based environment may be established, and necessary data and information may be securely migrated to that environment.

Incident Management Strategy Policy

DEA maintains a consistent approach to managing information security incidents in accordance with applicable laws and requirements.

Information security events and weaknesses will be addressed through procedures that include:

- Completely documenting reported security incidents.
- Preserving logs and other evidence of a security breach for review.
- Taking immediate measures to stop ongoing attacks when detected.
- Effectively communicating information security events and vulnerabilities to enable timely corrective action.

Incident Response

The Incident Response Plan outlines procedures for incident prevention, detection, assessment, forensic analysis, containment, and recovery.

The purpose of the plan is to mitigate computer security risks through comprehensive and structured responses to incidents.

Designated Incident Response Personnel

Designated personnel are responsible for responding to information security incidents and executing the procedures established in the Incident Response Plan.

Responsibilities include:

- Initial response.
- Investigation.
- Mitigation.
- Coordination with external experts when necessary.
- Documentation.
- Recovery.

Business Continuity Management Policy/System Failure

Backup and recovery plans are documented and made available to appropriate personnel in the event of a system failure or other disruption.

Procedures include:

- Reviewing and testing backup and recovery options regularly to ensure they continue to meet DEA's needs.
- Maintaining offsite backups and testing data recoverability.
- Regularly evaluating the physical security of electronic and hard-copy records.

Threat Assessment Policy

This policy is designed to help detect and prevent malware, phishing attacks, compromised credentials or passwords, sabotage, fire-related risks, and other threats.

Safeguards include:

- Antivirus protection through Webroot.
- Monitoring through Huntress.
- Anti-ransomware protection through Canauri.
- RMM monitoring.
- Firewall logs and updates.
- Onsite and offsite backups for disaster recovery.

Records Policy

This policy establishes protections for records and stored information.

Information may be classified as restricted, private, or public depending on its nature.

Examples include:

- School financial records – Restricted.
- Student financial records – Private.
- Tax information – Restricted.
- Loan applications – Restricted.
- Employee HR information – Restricted.
- Employee contact information – Private.
- Student contact information – Private.
- Student account balances – Private.
- Website content – Public.
- Student personal information – Private.
- Parent personal information – Private.
- Client personal medical information – Private.
- Student financial aid information – Private.
- Student grades and attendance – Private.
- Emergency contact information – Private.
- Student paper files – Private.
- Student digital files – Private.

Security procedures include:

- Applicable security scanning.
- Annual penetration testing.
- Continuous security monitoring.
- Security Operations Center (SOC) review of potential incidents.
- Removal or isolation of network devices when necessary.
- Antivirus protection through Webroot.
- RMM monitoring.
- Ransomware detection and response through Canauri.
- Appropriate security protections for data maintained on servers and within SMART.

Disposal

DEA requires all paper containing customer information to be shredded or otherwise securely destroyed before disposal.

When personal computers or other devices containing customer information are recycled or repurposed, memory components and storage media must be securely reformatted, erased, or destroyed as appropriate before reuse or disposal.

Monitoring and Detection

Institutional data and computing resources must be continuously monitored to detect events that may compromise their security.

Monitoring includes system, security, and operational events and is designed to allow DEA to identify potential security incidents promptly and effectively.

Commitment to Continuous Improvement

DEA is committed to continually improving its information security and incident response capabilities.

This includes regular reviews and updates to the Data Privacy, Cyber Incident & Information Security Response Plan and appropriate training for incident response personnel to ensure preparedness for new and evolving threats.

Audits and Monitoring

DEA reserves the right to conduct periodic audits and random compliance checks.

Continuous monitoring of networks and systems will be used to support compliance with the institution's cybersecurity policies.

Handling Non-Compliance

Non-compliance with this policy must be reported to the Director of Operations.

DEA will assess:

- The nature of the non-compliance.
- Potential risks involved.
- Necessary corrective actions.
- Measures needed to prevent future occurrences.

When necessary, the matter may be escalated for further review and appropriate action regarding the individuals involved.

Incident Reporting and Investigation

All actual or suspected information security breaches must be immediately reported to designated personnel.

Designated personnel are responsible for initiating an investigation and working with relevant internal and external parties to address the breach.

Reporting and management of breaches must follow the procedures established in the Incident Response Plan.

Disciplinary Actions

Individuals found to have violated this policy may be subject to disciplinary action.

Depending on the nature and severity of the violation, disciplinary measures may include:

- Loss of computer or network access.
- Loss of system privileges.
- Reprimand.
- Suspension.
- Termination of employment.
- Legal action, when appropriate.

Disciplinary measures will be applied consistently and in accordance with DEA policies.

Compliance Training

DEA will provide regular information security training and awareness programs to staff.

Training will address:

- The importance of information security.
- Requirements established by this policy.
- Individual roles and responsibilities.
- Appropriate handling of protected information.
- Identification and reporting of potential security incidents.

Insurance to Cover Data & Information Policy

CNA Data Breach Response Expense Policy and Procedure

Under applicable insurance coverage, CNA may pay eligible data breach expenses incurred by DEA as a result of a covered data breach involving personally identifiable information, subject to the terms and conditions of the applicable insurance policy.

In the event of a covered loss, DEA must follow applicable policy requirements, which may include:

- Reporting the data breach within the time required by the applicable insurance policy.
- Immediately documenting the specifics of the data breach and the date it was discovered.
- Cooperating with the investigation.
- Assisting the insurer, upon request, with enforcement of applicable rights against persons or organizations that may have accessed, stolen, or disclosed protected information.
- Obtaining required consent before voluntarily making payments, assuming obligations, or incurring covered expenses.

As soon as reasonably possible, DEA should provide the insurer with available information regarding the breach, including:

1. The method of the data breach.
2. The approximate date and time of the data breach.
3. The approximate number of files or records compromised.
4. A detailed description of the type and nature of the compromised information.
5. Whether the information was encrypted and, if so, the level or method of encryption.
6. Whether law enforcement has been notified.
7. If available, the applicable location or domicile of individuals whose PII was affected.
8. If available, information regarding who received or accessed the compromised information.
9. Other information or documentation reasonably required to investigate or adjust the loss.
10. Actions taken to protect PII remaining in DEA's care, custody, or control.
11. Preservation of evidence related to the data breach.
12. Other information, records, statements, or cooperation required under the applicable insurance policy.

CNA Data Breach Defense Policy and Procedure

CNA may pay covered losses on behalf of DEA resulting from a covered data breach claim, subject to the terms, conditions, exclusions, and reporting requirements of the applicable insurance policy.

DEA's responsibilities may include:

- Timely reporting of data breach claims.

- Cooperating with investigations, settlements, and defenses.
- Assisting the insurer in enforcing applicable rights of recovery.
- Executing necessary documents.
- Preserving evidence.
- Taking reasonable steps to protect PII remaining in DEA's care.
- Obtaining appropriate authorization before voluntarily making payments, assuming obligations, or incurring covered expenses.

DEA maintains crisis-management and incident-response resources through Electronic Brain Solutions and applicable insurance providers to assist with data breach response, notification, investigation, and recovery.

Continuing Evaluation and Adjustment

The Information Security Program will be reviewed annually by DEA's boards, staff, and third-party IT provider and will be subject to periodic review and adjustment as necessary.

Continued administration, development, implementation, and maintenance of the program are the responsibility of the designated Information Security Program Coordinator.

The Coordinator may assign specific responsibilities for technical, logical, physical, and administrative safeguards as appropriate.

Additional Definitions

Covered Data and Information

For purposes of this program, "covered data and information" includes student financial information protected under GLBA.

As a matter of DEA policy, this definition may also include other sensitive data, including credit card information and checking or banking account information received by the school, whether or not the information is independently covered by GLBA.

Covered data and information includes both paper and electronic records.

Pretext Calling

"Pretext calling" occurs when an individual attempts to improperly obtain personal information concerning an DEA customer, potentially for purposes such as identity theft.

This may involve contacting the school while falsely posing as the customer or as another individual authorized to receive the customer's information and using deception to persuade an employee to release protected information.

Student Financial Information

“Student financial information” means information obtained by DEA from a student or customer in the process of offering or providing a financial product or service, or information provided to the school by another financial institution.

Financial products or services may include student loans, financial aid services, and the collection of financial information necessary to administer financial aid.

Examples of student financial information include:

- Addresses.
- Telephone numbers.
- Bank account numbers.
- Credit card account information.
- Income information.
- Credit histories.
- Social Security numbers.
- Other protected financial information maintained in paper or electronic form.

Data Breach

A “data breach” means the loss, theft, accidental release, or accidental publication of personally identifiable information, or circumstances that objectively create a substantial risk that such loss, theft, release, or publication has occurred.

Data Breach Expense

“Data breach expense” includes eligible expenses associated with notifying individuals whose personally identifiable information was affected by a data breach, subject to applicable statutes, regulations, and insurance coverage.

Loss

“Loss” may include covered civil awards, settlements, judgments, applicable interest, and eligible expenses incurred in the defense of a regulatory proceeding, subject to applicable insurance terms.

Regulatory Proceeding

A “regulatory proceeding” means an investigation, demand, proceeding, or request for information brought by or on behalf of an applicable governmental or regulatory entity concerning a data breach.

Regulatory References

- Federal Trade Commission regulations: **16 C.F.R. Part 314**

- Gramm-Leach-Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- Applicable U.S. Department of Education Federal Student Aid information-security requirements
- Applicable federal and state data privacy and breach-notification requirements