HEADMASTERS
SCHOOL OF HAIR DESIGN

Student Information & Security Program

Compliance with the Gramm-Leach-Bliley Act
Financial Privacy Rule & Safeguards Rule

SAFEGUARDING THE PERSONAL IDENTIFIABLE INFORMATION OF OUR STUDENTS & THE SECURITY OF OUR SCHOOL

We take the security of all student sensitive information seriously at Headmasters School of Hair Design. To ensure necessary privacy and confidentiality, we have established guidelines that you will need to follow during your daily activities. This applies to physical and digital data.

WHAT IS "PII" & "FERPA"?

The Family Educational Rights Privacy Act (FERPA) is a Federal law that protects the privacy of student educational records. FERPA defines PII as Student Personal Identifiable Information. It includes direct identifiers (such as the names of a student and family members) and indirect identifiers (such as the student's date of birth, place of birth, or mother's maiden name).

Each student has a "Student File" that has the student's PII in it. Please protect this information. All Employees must remain mindful to not leave a student's file laying out on a desk where others can see the information. The student's file should remain in the Financial Aid Office or in the Director of Admission's Office if needed upstairs.

HOW YOU CAN PHYSICALLY KEEP OUR INFORMATION SAFE AND SECURE?

1. Considering physical barriers that stop access to information is always a good practice.
2. Offices should always be locked when employees with PII are not present. Doors to office areas should also be locked during non-business hours.
3. Student information is to be processed behind closed doors or in other areas not regularly accessible to the public or other students.
4. Passwords, user IDs, and PINs are not to be posted near or on computers.
5. Sensitive paper documents should be shredded on campus.

HOW DO WE PROTECT INFORMATION DIGITALLY?

1. Upon hire, you are assigned a unique headmasters.edu email address. You will also be given a passcode for it.
2. Please minimalize active computer screens while stepping away, so that data cannot be viewed by unauthorized individuals. Please log off when you will not be using the device.
3. Do not open suspicious emails or click on links that are questionable. Here are some general tips for checking link safety. If a link looks suspicious, do not click it. Access the service through its official URL, not random buttons, images, or links. Odd characters in links could suggest URL encoding used to mask harmful destinations or fake websites. If an URL features HTTP instead of HTTPS, it should discourage you from revealing any personal information. Quickly report possible breaches or unusual computer behavior Tracy or Kris. They may have a technician work to safeguard our information and data. May need to have Subterranean back up the server.

FAMILY EDUCATION RIGHTS AND PRIVACT ACT (FERPA)

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C.s 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students".

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible to parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR s 99.31):

1. School officials with legitimate education interest;
2. Other schools to which a student is transferring;
3. Specified officials for audit or evaluation purposes;
4. Appropriate parties in connection with financial aid to a student;
5. Organizations conducting certain studies for or on behalf of the school;
6. Accrediting organizations;
7. To comply with a judicial order or lawfully issued subpoena;
8. Appropriate officials in cases of health and safety emergencies; and
9. State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

Headmasters School of Hair Design is required to:

- Annually notify students of their rights under FERPA;
- Under FERPA, a school is required to provide a student with an opportunity to inspect and require his or her education records within 45 days of the receipt of a request; and
- Headmasters School of Hair Design will provide copies of education records, or make other arrangements to provide the student access to the records upon request to the student or parent.

I have read and understand my rights regarding the FERPA requirements of the school and myself.

_____	_____	_____
Student Signature	Print	Date

Headmasters School of Hair Design

RELEASE OF STUDENT INFORMATION

I understand that I have the right to gain access to my records according to the school's Access to Files Policy by making an appointment with the appropriate school official.

I also understand that I have the right to authorize certain individuals, organizations, or class of parties (such as potential employers) to gain access to certain information in my student file.

I hereby authorize _____ to have access to the following information:

_____
_____
_____
_____
_____
_____

_____ _____ _____

Signature Print Date

Note: This form is to be used each time the school wants or has a need to release information from the student file to a third party.

This form need not be used when releasing information from the student's file to the student or student's parent if the student is a dependent student under IRS laws.

SAFEGUARDING CUSTOMER INFORMATION

August 1, 2015

1. Introduction

Headmasters is committed to protecting the privacy of non-public customer information. The purpose of this policy is to describe Headmasters' policies and procedures for complying with the specific requirements set forth in the federal Gramm-Leach-Bliley Act (GLB Act).

This policy describes how Headmasters protects information specifically covered under the GLB Act.

1.1 Summary of Requirements of GLB Act

The GLB Act requires "Financial Institutions," defined below, to protect non-public personal information that is collected from an individual who obtains or has obtained a financial product or service from the institution for personal, family or household purposes.

Financial products or services offered by Headmasters and covered by the GLB Act include, but is not limited to:

- Student loans

Examples of information that would require protection include tax returns, Social Security numbers or other non-public or personal information that is collected for purposes of providing these services.

The safeguarding regulations of the GLB Act ("Safeguards Rule") require that covered institutions, such as Headmasters, develop, implement and maintain a comprehensive information security plan that includes administrative, technical and physical safeguards to protect the information covered by the GLB Act. The plan must describe how Headmasters protects customer information.

2. Definitions

2.1 Financial Institution

An institution significantly engaged in financial activities, which include:

- lending, exchanging, transferring, investing for others, or safeguarding money or securities. These activities cover services offered by lenders, check cashers, wire transfer services, and sellers of money orders.
- providing financial, investment or economic advisory services. These activities cover services offered by credit counselors, financial planners, tax preparers, accountants, and investment advisors.
- brokering loans.
- servicing loans.
- debt collecting.
- providing real estate settlement services.
- career counseling (of individuals seeking employment in the financial services industry).

2.2 Financial Product or Service

A financial product or service covered under the GLB Act includes the following:

- offering student, faculty or staff loans;
- making, acquiring, brokering, or servicing loans or other extensions of credit;
- real estate and personal property appraising;
- arranging commercial real estate equity financing;
- collection agency services; and
- credit bureau services.

2.3 Consumer

Someone who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family or household purposes, or that person's legal representative. Examples include:

- making a wire transfer; or
- applying for a loan, whether or not the individual actually obtains the loan.

2.4 Customer

Customers are consumers who have a continuing relationship with a financial institution. Examples include:

- receiving loan disbursements from a financial institution;
- opening a credit card account with a financial institution; or
- using the services of a mortgage broker to secure financing.

2.5 Non-Public Personal Information

Any personal identifiable financial information that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available. Examples include:

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

3. Policy

Headmasters shall comply with the Safeguards Rule, which requires the institution to:

- Designate one or more employees to coordinate the program;
- Identify "reasonably foreseeable" internal and external risks to the security and confidentiality of customer information that could lead to unauthorized disclosure, use, alteration, destruction or other compromise of such information and "assess the sufficiency" of the institution's safeguards in place to control these risks.

  Such risk assessment must include, at a minimum, risks in areas of operation such as:
  - Employee training and management,
  - Information systems, and
  - detecting, preventing, and responding to attacks against the institution's systems;
- Implement safeguards to manage the identified risks and regularly test or monitor such safeguards;
- Oversee the institution's service providers by:
  - Selecting and retaining service providers that are capable of maintaining appropriate safeguards for the customer information at issue, and
  - Requiring service providers by contract to implement and maintain such safeguards; and
- Evaluate and adjust the institution's security program in light of such risk assessment, any material change to institutional business operations or any other circumstances that may have a material impact on the institution's information security program.

Section 4.0 of this document describes the procedures for implementing the above policy.

4. Procedures

4.1 Employee Designation

Headmasters' Financial Aid Administrator is responsible for the Safeguards Rule of the GLB Act. The following offices will specifically assist in protecting data covered by the GLB Act:

- Dusty Peterson, Secretary/Owner
- Kris Massey, Instructor

4.2 Risk Assessment

Headmasters units that may be impacted by the Safeguards Rule of the GLB Act include, but are not limited to:

- Financial Aid,
- Registrar's office, and
- Student Financial Services

Each of these units continues to implement security procedures to comply with the GLB Act.

4.3 Training

All users of the Student Information Systems (SIS) must sign Confidentiality Agreements, acknowledging their respective responsibilities to maintain the confidentiality of student information.

4.4 Implementing Safeguards

Headmasters already has some formal policies and procedures that address information security of the data covered by the GLB Act as well as consequences for failing to maintain the confidentiality of certain information, including:

- Family Educational Rights and Privacy Act (FERPA) policy,
- Misappropriation of Assets,

Headmasters information security program incorporates the following safeguards, as appropriate:

- Locking rooms where paper records are kept,
- Ensure that storage areas are protected against destruction or potential damage from physical hazards,
- Using password-activated screensavers,
- Using strong passwords,
- Storing electronic customer information on a secure server,
- Maintain secure backup media and keep archived data secure,
- Changing passwords periodically,
- Encrypting customer information when it is transmitted electronically over networks or stored online, when possible,
- Referring calls or other requests for customer information to designated individuals who have had appropriate training for addressing such requests,
- Reporting incidents of fraudulent or suspicious attempts to obtain customer information,
- Disposing of customer information in a secure manner, such as shredding or erasing data when disposing of computers and recycling,

4.5 Security Data Breach

What is an Information Security Data Breach?

A type of incident which includes the access, use, theft, loss of control, disclosure and/or distribution of sensitive data (e.g. SSN, DOB, student grades, tax records, credit card information) in violation of a law or regulation.

An information security data breach incident may involve any or all of the following:

- A violation of Federal data privacy laws (FERPA, GLBA), Headmasters School of Hair Design System information security policies and procedures.
- Unauthorized data access by an employee or external entity.
- Unintended disclosure of, loss of, or altered sensitive data.
- Presence of a malicious application, such as a virus or malware, that impacts sensitive data.
- Credentials or other access control mechanisms that are lost, stolen, or disclosed.
- Lost or stolen computing devices that contain sensitive data.
- Lost or stolen mobile storage devices that contain sensitive data.

Data Breach Assessment, Prioritization, and Response

The person who discovers the data breach will immediately report it to the owner, Dusty Peterson. Dusty will immediately convene a team to perform the following steps:

I. Validate the data breach:
   - A. Has a data breach occurred in violation of a law or regulation?
   - B. Is the status of the data breach active or post breach?
   - C. What was the method of data disclosure?

a. Internal, external, malicious, accidental/unintended?

D. Does the breach impact system functionality?

E. To what extent does the breach affect faculty, staff, and students?

F. What is the anticipated reputational and financial impact to the school?

II. Assign a high or low priority level to the data breach based on current and future impact.

III. Notify Owners of high priority data breaches.

A. Owners, with guidance from legal counsel, will determine whether to notify law enforcement based on the nature of the breach and federal, state regulations.

B. Owners will designate a school representative with the authority to share breach information to external parties including law enforcement.

IV. Notify data owners and identify all affected data, machines, and devices.

V. Follow applicable FERPA guidelines.

VI. Document and report on breach response activities and coordinate the flow of information about the breach to School employees.

VII. Locate and preserve (when possible) all written and electronic logs and records applicable to the breach for examination.

VIII. Work with data owners and IT to mitigate damage and determine the root cause of the breach to prevent future occurrences.

IX. Determine when to notify affected faculty, staff, students, and authorized third parties with guidance from Owners and external Legal Counsel.

A. Law Enforcement will provide notification guidance if the breach is under criminal investigation.

X. Create an appropriate media notification after approval from Owners, and external Legal Counsel, and Law Enforcement.

XI. Perform a final assessment of the data breach and ensure that controls are in place to prevent a reoccurrence. Notify Team of low level data breaches after final assessment is complete.

Data Breach Response Phases (Reference)

1. Identification
2. Notification to response team
3. Assessment
4. Containment
5. Eradication
6. Recovery
7. Documentation
8. Notify external agencies and customers (if warranted)
9. Remediation
10. Lessons learned

4.6 Use of Information Technology Resources

Purpose

This policy governs Headmasters School of Hair Design employees use of information technology (IT) to securely access, maintain, and transmit Headmasters data and access the internet in compliance with local, state, and federal laws.

Definitions

1. Information Technology – college owned, licensed, or subscription-based computing and communication resources that manipulate, store and transport all data types and formats.
2. User – Full and part-time Headmasters employees or any other authorized individuals using School owned, licensed, or subscription-based information technology.

Acceptable Use

Users are responsible for reviewing and complying with all policies and procedures related to acceptable use and security of IT resources. Access to mobile computing devices, computer systems, and networks owned or operated by the State of Idaho imposes certain responsibilities and obligations on users and is subject to state government policies and local, state and federal laws. Acceptable use of information technology must be ethical, professional and responsible in the consumption of shared IT resources. Acceptable use demonstrates respect for intellectual property, privacy and ownership of information, system security and freedom from intimidation and harassment.

System Usage

1. Information Systems Training -All users must complete in person software training before accessing the Premiere student database.
2. Personal Use – Headmasters School allows employees to make reasonable personal use of its electronic mail, internet access, and other computer and communications systems provided it does not interfere with business activities or IT resource availability. IT resources may not be used to support a personal business or similar personal ventures.

User IDs and Passwords

1. User IDs - Users are responsible for all activity performed with their personal user IDs. They must not permit others to perform any activity with their user IDs, and they must not perform any activity with IDs belonging to other users.
2. Password and Access Code Sharing Prohibited – Users must not disclose or share their Headmasters network passwords, and other access codes with other users.
3. Strong Passwords – Users must choose passwords that are difficult to guess and meet system password requirements. Users must not choose derivatives of user IDs, common character sequences, personal history details, a common name, or a word that reflects work activities. Users should create unique passwords for different sites, programs, and devices.
4. Password Proximity to Access Devices - Users must never write down or otherwise record a readable password and store it near the computer or device to which it pertains.
5. Typing Passwords When Others Are Watching - Workers must never type their passwords at a keyboard or a telephone keypad if others are watching their actions.

Electronic Messaging and Videoconferencing

Headmasters prohibits the following. Users must not:

1. Forge or manipulate message author information.

2. Distribute spam, computer viruses, malware, or other harmful software programs.
3. Send messages or transmit audio/video containing inappropriate content deemed threatening, discriminatory, defamatory, obscene, or prohibited by local, state, and federal law.
4. Send unencrypted, plain text e-mail and text messages containing protected, sensitive data (Social Security Numbers (SSNs), credit card numbers, Date of Birth (DOBs), student records, tax information) to external recipients.
    a. Users must encrypt sensitive data in message file attachments or securely upload sensitive data to external websites and portals.
5. Request that Headmasters students and the public email or text sensitive data via unencrypted plain text messages to Headmasters accounts.
6. Send internal email messages containing sensitive employee or student data. Users must redact or mask sensitive data.
7. Click on links or file attachments in messages that are in any way suspect and potentially malicious without verifying message authenticity.

Network and Internet Access

1. Activity Monitoring – Users must be aware that their network and internet activity, while using Headmasters systems or personally owned devices connected to Headmasters' network, may be monitored for business-related or security purposes.
2. Compliance Audit – Headmasters reserves the right to audit all devices on Headmasters networks, including personally owned devices, to ensure that each device complies with Headmasters policies and procedures.
3. Current Virus Software- Users must maintain current antivirus software on all personal computing devices that access Headmasters network.
4. Unattended Active Sessions - Users must not leave their work computer without locking the desktop or logging out for security purposes.
5. Session Timeout – Computer desktops and other Headmasters devices must auto lock after a set period of inactivity.
6. Computer Viruses
    a. Any user who suspects infection by a virus or malicious software (malware) must immediately contact IT, and not attempt to eradicate the virus without assistance from IT.
    b. Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of Headmasters computers or network.
7. Use at Your Own Risk - Users access the Internet through the Headmasters network at their own risk. Headmasters is not responsible for material viewed, downloaded, or received through the Internet.
8. Appropriate Use – Users may not access networks for illegal or unlawful, or immoral purposes or to support or assist such purposes; for example, the transmission of violent, threatening, defrauding, obscene or otherwise illegal or unlawful materials.

Data Storage

1. Users must store Headmasters work files on the following resources:
    a. Departmental network drive
    b. OneDrive- (Microsoft secure Cloud storage)

2. Users should not store Headmasters work files on their local hard drive (C: drive). IT does not back up individual computer (laptop/desktop) hard drives.

Physical Security

1. Sensitive Information – Users must lock all hard copy sensitive information in file cabinets, desks, safes, or in a locked office.
2. Computing Equipment - A user must promptly inform the owner if a Headmasters computing device has been damaged, lost, stolen or is otherwise unavailable for work activities.
3. Use of Personal Equipment - Users must not bring their own computers, computer peripherals, network devices, or computer software into Headmasters without prior authorization from the owner.
4. Computing Equipment Checkout – TTC computing devices must not leave Headmasters unless properly authorized and secured.

Security Incident Reporting

Users must report any suspected events that may compromise information security or violate an existing information security policy to the owner. Examples of these events include:

- Any unauthorized use of Headmasters information systems.
- Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed.
- All unusual systems behavior, such as missing files, frequent system crashes, and misrouted messages.
- Suspected or actual disclosure of sensitive Headmasters information to unauthorized third parties. Please refer to Headmaster's data bread plan.
- Lost or stolen Headmasters computing devices.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. This agreement does not preclude enforcement under laws and regulations of the State of Idaho and the United States of America. Headmasters reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Headmasters does not consider conduct in violation of this policy to be within an employee's course and scope of employment, or the direct consequence of the discharge of the employee's duties. Accordingly, to the extent permitted by law, Headmasters reserves the right not to defend or pay any damages awarded against employees that result from violation of this policy. Any employee, who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her supervisor or the owner as soon as possible.

5. Resources

Federal Trade Commission:
http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html
U.S. Senate Committee on Banking, Housing and Urban Affairs: Information Regarding the Gramm-Leach-Bliley Act of 1999
http://www.senate.gov/~banking/conf/
National Association of College and School Business Officers: 2003-01 Colleges and Universities Subject to New FTC Rules Safeguarding Customer Information (January 13, 2003)

(Effective July 12, 2022, the following was implemented with the previous information)

Gramm-Leach-Bliley Act
The Bramm-Leach-Bliley Act (GLBA) was passed by Congress in 1999 and is enforced by the Federal Trade Commission. It is a federal law that protects customer's non-public information, otherwise known as NPI. Examples of NPI include social security numbers, credit card numbers, tax return information, driver's license, and dates of birth. This also includes student financial aid records and information.

FLBA is comprised of two categories: the Financial Privacy Rule and Safeguards Rule.

Financial Privacy Rule
An institution achieves compliance with the Financial Privacy Rule when FERPA rules are established and maintained. Headmasters School of Hair Design acknowledges and practices all FERPA guidelines as posted on our website in our Student Catalog at https://www.headmasters.edu/media/Student-Catalog.pdf. (Please see attached FERPA document that is signed by students in orientation.)

Safeguards Rule
Higher education institutions, such as Headmasters School of Hair Design, are also subject to the Safeguards Rule Act. This Rule addresses the administrative, technical and physical safeguarding of consumer information. We are required to take necessary precautions to ensure the privacy, security, and confidentiality of customer and student records. A Securityu Program is required. Headmasters School has implemented a Program to comply with the Gramm-Leach-Bliley Act (GLBA). This Program safeguards student and financial information, as well as all non-public information in paper and electronic form, regarding various Federal and state laws and other authorities, including the HEA; the Family Educational Rights and Privacy Act (FERPA); the Gramm-Leach-Bliley Act; state data breach and privacy laws; and potentially other laws.

The Headmasters School of Hair Design Program seeks to (1) ensure the security and confidentiality of customer and student records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer or student. This program is a plan to assess existing risks to customer or student information including ways to manage and control the existing risks. Our plan also monitors third-party outsourcing arrangements to ensure compliance with the college's policies and procedures. Twelve main components comprise our Security Program.

Security Program Components

a. **Designate a "Qualified Individual" responsible for overseeing, implementing, and enforcing the information security program.** Tracy Waffle has been designated as the "qualified individual" to oversee, implement and enforce the information Security Program. She also communicates and oversees our IT provider TurnKey, 208-743-0356 or Patrick with TurnKey at 208-848-6694.

b. **Base the information security program on a risk assessment of the security, confidentiality, and integrity of customer information, and assess the sufficiency of any safeguards in place to control these risks.** Headmasters School's information security program follows a risk-based approach as outlined here:

Risk Management

Headmasters School protects the confidentiality, integrity, and availability of its information assets while balancing the needs of teaching and learning. Turnkey provides information security strategy, vision, and coordination. Heads of Headmasters School are responsible for the risks associated with their assets. Information security is everyone's responsibility.

The information security program's risk-based approach to cybersecurity supports Headmasters by balancing risks and creating situational awareness about critical information assets and associated threats. We examine real conditions while remaining adaptable and nimble in our practices.

Risk Management Practices

- Adopt a repeatable risk management framework for reporting and prioritizing work efforts.
- Document and assess the value of critical data assets, technology services, people, business relationships, and partners.
- Prioritize assets and related risk-mitigation efforts based on available resources.
- Establish clear responsibility and communication plans for information security, including incident response.
- Enable innovation and control contract risk with fair, clear, and practical terms and conditions that reduce liabilities related to asset loss or compromise.
- Implement an intelligence program based on reliable sources for evolving threats, incidents, industry trends, adversary profiles, and related analysis.
- Establish a network of trusted strategic partners and experts, including our campus Security Advocates.
- Implement incident response and management capabilities.
- Minimize the electronic attack surface and vulnerabilities for all critical assets.
- Implement tools and procedures to respond to and defend against intrusions

The components of the program are established here:

Security Plan

The Heads of Headmasters are responsible for the risks associated with their assets. They must document and implement an Information Security Plan (Plan) that demonstrates due care in securing their assets by meeting the intention of the controls in this policy statement. The Plan must address each of the requirements in this policy statement and include the following:

- Include a Plan implementation timeline and milestones
- Describe the organization's approach to implementing the Plan
- Document critical assets and the controls that are implemented for each of them
- Describe alternate or compensating controls and the rationale for selecting them.

General Operational Controls

General operational controls include the appropriate security controls and operational practices for Headmasters networks, information systems, applications, and information throughout the school. These controls must be defined, implemented, maintained, and include the following:

- A change and configuration management process
- A flaw remediation process
- A malicious code and unauthorized software countermeasure process
- A data protection and destruction process
- Secure development practices
- Backup and recovery processes for critical information and software
- A business continuity and disaster recovery plan
- Information security technical architecture standards
- System build and maintenance standards
- Acceptable use standards.

Physical Controls

Physical controls define the protection required for the data center, physical assets, critical information systems, and institutional information. These controls must be defined, implemented, maintained, and include the following:

- Physical protection and access processes for buildings that house critical information technology and systems
- A physical protection process for critical information systems and institutional information.

c. **Design and implement safeguards to control the risks identified in the risk assessment.** Headmasters School has established standards that applies to Confidential data in the form of the "Release of Student Information" form and FERPA, and also including data in the scope of GLBA. If additional safeguards are needed to address identified risks, the Information Security Program will work directly with the employee/person, as needed, to address the risks. Employees must use a multi-factor authentication (MFA), once for computer login and again to login to each program. Subterranean does a network backup every evening from off campus and, therefore, the information is stored off campus. Our website (headmasters.edu) is secured, and the

SSL certificate is updated annually. The SSL is a digital certificate that authenticates a website's identity and enables an encrypted connection. The digital certificates are rotated and updated every three months and it provides secure submissions of forms. Webhosting is provided by KLM Graphics.

d. **Regularly test or otherwise monitor the effectiveness of safeguards.** For information systems, the monitoring and testing shall include continuous monitoring or yearly penetration testing and vulnerability assessments.
e. **Implement policies and procedures for security awareness training.** People who have access to GLBA data are required to take GLBA training and information security training at least annually. Go to https://www.youtube.com/watch?v=yYLg0FIXyoA to watch the training. Turn in an attestation to Tracy after you have watched it with a note saying you watched the GLBA training webinar and your name and the date.
f. **Oversee service providers.** Must sign a confidentiality form.
g. **Evaluate and adjust the information security program** in light of the results of testing and monitoring. Headmasters regularly reviews and adjusts the information security program following established governance practices.
h. **Establish an incident response plan.**

Incident Reporting and Management

Workforce members must report an unforeseen event, a potential or confirmed breach of personal data, or an information security incident promptly to the office responsible for responding to and/or managing the incident as noted in this policy.

- Report by workforce members;
- Assignment of an incident manager;
- Identification and preservation of evidence;
- Assessment of risk to the institution, potential harm to individuals, and compliance with applicable laws and regulations;
- Containment action(s) to stop harm caused by the incident, if any;
- Communication plan(s);
- Mitigation effort to address the weakness that caused the incident;
- Recovery or restoration of the affected system(s) or service(s) back to an operational state; and
- Management of records according to the applicable records retention schedule.

i. Require your Qualified individual to report in writing, regularly and at least annually, to the owners.
j. If you suspect you may have been compromised or had a breach, **report a breach** with the Cybersecurity Intake Form, https://fsapartners.ed.gov/title-iv-program-eligibility/cybersecurity/cybersecurity-breach-intake.