CARIS COLLEGE

PATIENT CARE CAREERS

GLBA Information Security Program

Published June 9, 2023

Table of Contents

Introduction

Caris College's Information Security Program (ISP) is intended to describe the safeguards implemented by the institution to protect confidential information (both electronic and physical) in compliance with the Gramm-Leach-Bliley-Act (GLBA) Safeguards Rule. Issued by the Federal Trade Commission (FTC), the Safeguards Rule is designed to:

- Ensure the security and confidentiality of student information
- Protect against any anticipated threats or hazards to the security or integrity of such information
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any student

To that effect, the institution developed the ISP to aid in the identification and prevention of such threats. The ISP describes Caris College's safeguards to protect confidential information and provides mechanisms to respond to such a threat in the event of an occurrence through risk assessment practices, written policies and continuous system review.

Oversight

The President of Caris College serves as the Qualified Individual (QI) who coordinates the development and implementation of the college's Information Security Program (ISP). In this role, the QI is supported by a committee of individuals who work together to ensure the plan is effective by:

- Examining risk assessment practices and results
- Implementing policies to address weaknesses
- Identifying appropriate responses to a potential data breach
- Developing safeguards to prevent future occurrences
- Reviewing of ISP to ensure effectiveness of the plan

The committee meets on an annual basis to formally evaluate the ISP and make necessary changes. Committee members, along with other pertinent individuals, also make up the Incident Response Team (IRT). While members may transition at times, the committee primarily consists of individuals in the following roles: Academic Leadership, Administrative Leadership, Student Recordkeeping, Financial Aid. Representation from each area is critical to the success of the ISP. The QI compiles data and pertinent information from the annual ISP evaluation and shares it with stakeholders of the institution for additional review.

Risk Assessment

Caris College recognizes that the college is exposed to both internal and external risks of unauthorized use or access to confidential data. Examples of such risks, include, but are not limited to:

- Unauthorized access of confidential information by someone other than the owner of the confidential information.
- Compromised system security because of system access by an unauthorized person.
- Interception of data during transmission.
- Loss of data integrity.
- Physical loss of data in a disaster.
- Errors introduced into the system.
- Corruption of data or systems.
- Unauthorized access to confidential information by employees, students, or affiliates.
- Unauthorized requests for confidential information or covered data.
- Unauthorized access through hardcopy files or reports.
- Unauthorized transfer of confidential information through third parties.

At Caris College, data is classified into 4 levels, with each subsequent level requiring less security:

Data Security Level	Definition	Example(s)
Level 1: Confidential	Data in which access by unauthorized parties could cause the College to incur substantial losses	1. Social Security Number in combination with an individual's name. 2. Mission-critical information defined by the College that is critical to its continued performance. 3. Budget and information about major transactions. 4. College partnerships or contracts.
Level 2: Regulated Information	Data that is governed by regulatory restrictions and is forbidden to show or discuss with unauthorized parties.	1. Educational records; according to Family Educational Rights and Privacy Act (FERPA). 2. Health information; according to the Health Insurance Portability and Accountability Act (HIPAA).
Level 3: Internal Use	College-related information that is accessible only to those who need this information for their specific job responsibilities.	1. Internal emails 2. Internal policies and procedures
Level 4: Public	Readily available information in the public domain.	1. Marketing for a program offered by the College. 2. Presentations approved for external use. 3. School catalog and other files posted on the College's website.

Caris College recognizes that this may not be a complete list of the risks associated with the protection of confidential information. Since technological growth is dynamic, new risks are created regularly and the College will actively monitor cybersecurity advisory groups as well as industry sources for identification of risks.

Caris College believes that the currently implemented and monitored safeguards are reasonable and are enough to provide security for confidential information maintained by the College. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

Safeguards Design

The designed safeguards are regularly assessed to evaluate their effectiveness in controlling the risks the College may be exposed to. Below, we present some scenarios for these risks and the safeguards in place to control/eliminate such risks:

1. **Employee training:**

   Scenario 1*: *Risk: New employees are not aware of the College's policies and practices to protect students' information from external or internal risks.

   Safeguard: All new employees complete training within the first 60 days of employment. Training opportunities on topics such as cybersecurity awareness are available on the College's online training platform, Vector Solutions. Sufficient tracking mechanisms are in place to notify the managers if a new employee has not completed the required modules.

   Scenario 2*: *Risk: An employee shares the reason for a student's dismissal with a parent that did not sign the FERPA release form.

Safeguard: All employees receive extensive training on data classification and the security level associated with each category, as well as the parties the information could be shared with.

2. **Technical and Physical safeguards of the Information systems:**

   ***Risk*:** An employee downloads a student's personal data to a laptop to work at home without following current policies.

   ***Safeguard*:** In addition to the training opportunities on the College's online training platform, Vector Solutions, that increase the awareness of data confidentiality, we are seeking to secure additional training platforms to ensure that employees follow proper protocols while working with confidential, regulated, and internal-use data.

3. **Detecting, preventing, and responding to attacks against the College's systems:**

   ***Risk*:** Systems need to be monitored and tested to ensure students' and employees' data is protected from internal or external compromise.

   ***Safeguard*:** The College is adopting current practices that include firewalls, anti-virus protection, and activity logs that are sufficient to control risks on all computers on campus. Anomalies in logs are reviewed to detect possible security issues.

Safeguards Implementation

Employee Training

The successful design and implementation of safeguards to control risks identified through the risk assessment begins with appropriate training. At the point of hire, Caris College employees are assigned a series of training sessions aimed at educating them on the importance of protecting confidential information and the risks of security breaches. Training sessions are maintained in the institution's online training platform, Vector Solutions. Vector Solutions provides prefabricated training sessions on a variety of topics, including cybersecurity awareness. The system allows administrators to assign training to employees and requires the successful execution of a training assessment before receiving a certificate of completion. Vector Solutions also allows the integration of external training files so that Caris College officials can manage the quality of content provided to employees. Finally, Vector Solutions provides recordkeeping functionality to track training progress and completion.

Policies and processes have been developed to promote the application of resources learned through the training process. Failure to comply with these policies may result in disciplinary action. In the event of a security breach, or if further information is needed, employees may be assigned additional training requirements through Vector Solutions in an effort to reduce the risk by promoting continual education in this area.

Physical Security

Initiatives are taken to prevent physical breach of confidential information. For example, Caris College adopts a "clean desk" principle - promoting the safe keeping of sensitive information by clearing workspaces of confidential paperwork, locking drawers and office doors when away, closing computer screens/locking computers when not in use, etc.

Additionally, employees identify documents containing sensitive information by marking them as *Personally Identifiable Information.* This identification is easy to notice as it is written in red and displayed in prominent areas on the document. Employees are trained to associate this marking as private information and treat it with confidentiality.

Access to sensitive information is restricted to those authorized to review it. Restrictions are identified by role and electronic/physical access is granted only to those roles deemed necessary. Access is managed by College officials and evaluated regularly.

Virtual Security

Caris College utilizes the following services to safeguard virtual systems from unauthorized use:

- Watchguard: Firewall protection
- Huntress: Security platform monitoring service
- Backblaze: File backup service

The institution also utilizes the protection of a two-factor authentication system to reduce the risk of security breaches. This system is used by all employees when accessing the network as well as all account holders when accessing Caris College's Student Information System, Populi. Additionally, outgoing email messages are encrypted to reduce the risk of interception of information. Policies for such processes are developed and shared with employees. Training materials/user guides are also provided. These areas are regularly monitored by college officials to ensure consistency in practices.

Third-Party Service Providers

Caris College makes every effort to ensure third party service providers adhere to safety protocols aimed at preventing the unauthorized access and use of sensitive information. Confirmation of such protocols are stored electronically for reference. If a servicer is unable to provide the requested information, Caris College will work with them to make this available. If it is impossible to provide, Caris College will discontinue the working relationship in favor of a servicer with appropriate security measures.

The institution utilizes the services of a third party non-biased provider to perform regular information security risk assessments and identify potential weaknesses. Weaknesses are addressed and new safeguards implemented to reduce the risk of an information breach. Additionally, the QI and ISP committee conduct internal reviews on a regular basis to promote safe practices and ensure the reduction of risk.

System Failure/Compromise

In the event that a safeguard or system fails, Caris College has processes in place to assess the impact and identify next steps. Potential next steps include, but are not limited to:

- Notify of risk
- Develop and execute action plan
- Take disciplinary action (if necessary)
- Install safeguards to prevent further failure/compromise
- Continually evaluate and adjust as needed

Policies and Procedures

Information Security is everyone's responsibility. All Caris College personnel and persons of interest (POIs) with access to confidential information, whether through use of online technology resources or otherwise, are covered by this administrative regulation. All personnel and POIs must complete training on the information security administrative regulations and information security awareness training annually, certify their attendance at each training session, and certify their familiarity with the institution's requirements for protecting confidential information in compliance with the ISP. Caris College students are expected to know and comply with all current published policies, rules and regulations as stated in the college catalog, class schedule, and/or student handbook.

Failure to comply with this administrative regulation may result in disciplinary actions up to and including dismissal from employment and termination of service at Caris College. Legal actions, including, but not limited to the application of civil and criminal penalties, may also be taken for violations of applicable regulations and/or laws.

Caris College recognizes that laws and regulations involving security of confidential information are continuously evolving. In this context, to the extent that applicable data privacy laws or regulations conflict with the procedures

outlined in the ISP, the applicable laws or regulations govern and override the ISP. Personnel and POIs should notify the QI immediately of applicable law or regulations that appear to conflict with the ISP.

Information security is everyone's responsibility. Listed below are some of the crucial roles and responsibilities associated with implementation of the ISP:

Role	**General ISP Responsibilities**
All	Report security incidents by exclusively contacting the QI bkepley@cariscollege.edu, without communicating with anyone else beforehand.
QI	Issue governance directives as needed to regulate use of IT resources and protection of confidential information. 1. Implement the ISP. 2. Regularly test the ISP's safeguards. 3. Facilitate compliance with regulatory requirements in coordination with Caris College IT and legal personnel. 4. Evaluate the ability of relevant Caris College personnel and POIs to implement and maintain appropriate security measures for the confidential information to which Caris College has permitted access and require such individuals to implement and maintain appropriate security measures. 5. Review the ISP, in collaboration with the Incident Response Team (IRT), at least annually and whenever there is a material change in Caris College's business practices that may implicate the confidentiality, integrity, security and/or availability of Caris College confidential information.[2] 6. Obtain details about the situation from the individual(s) who report actual or suspected security incidents. 7. Coordinate with the IRT to take any additional actions that may be appropriate.
Information Technology Consultant	1. Configure network devices to prevent possible electronic breaches. 2. Configure intrusion detection and file integrity monitoring systems to continually track activity and identify possible electronic intrusions.
Role	**Training, Awareness and Compliance Responsibilities**
QI	1. Conduct training that includes all Caris College personnel and POIs and those employed by others to perform Caris College work who regularly use and/or have access to confidential information 2. Maintain accurate records pertaining to all training activities.
Assistant Campus Director	1. In collaboration with the QI, provide training to all personnel and POIs via an online training course on the information security administrative regulations and information security awareness every year, and additional training as warranted.

Personnel and POIs	1. Complete training on the information security administrative regulations and information security awareness annually, certify completion of each training session, and certify familiarity with Caris College's requirements for protecting Information in compliance with the ISP.[4] 2. Maintain the confidentiality, integrity, security, and availability of Caris College confidential information in compliance with the ISP.[5] 3. Comply with Caris College standards, including, but not limited to, the acceptable computer use provisions described therein.[6]
Role	**Internal Risk Mitigation Responsibilities**
QI	Review and reevaluate information security measures annually or whenever there is a material change in Caris College's business practices that may reasonably implicate the security or integrity of records containing confidential information.
ISP Committee	Review and reevaluate, in collaboration with the QI, information security measures annually or whenever there is a material change in Caris College's business practices that may reasonably implicate the security or integrity of records containing Confidential Information.
Institutional Management	1. Obtain acknowledgement, via the completion of the required online training course, that all personnel and POIs have received a copy of the ISP and will abide by its provisions. 2. Require that responsible parties at all Caris College sites work with the QI to establish exit processes that require personnel and POIs who cease employment/contract service with Caris College ("Separated Individuals") to return all records, data applications and/or systems, in any form, including, but not limited to, information stored on laptops or other portable devices or media, and in files, records, and work papers, and surrender all keys, identification cards, and all other means of using and/or accessing Caris College's premises and/or information.
Management through enforcement of Administrative Regulations	1. Require that personnel and POIs immediately report any suspicious or unauthorized use of confidential information to the QI who coordinates with the IRT to appropriately respond. 2. Require that personnel and POIs who violate the ISP may be disciplined according to the severity of the violation, regardless of whether confidential information was accessed or used without authorization. 3. Require that all employment and consulting agreements contain provisions that (1) require all personnel and POIs to receive training and acknowledge, sign and comply with the provisions of the ISP, and 4. prohibit any nonconforming use of Confidential Information during or after employment. 5. Authorize in writing any and all exceptions to internal risk mitigation responsibilities
Information Technology Consultant	At the direction of the appropriate manager, revoke separated individuals' physical, electronic, and remote electronic use of and/or access to confidential information.

Personnel and POIs	1. Cooperate with efforts underway to limit the amount of confidential information collected or stored to that amount reasonably necessary to accomplish Caris College's legitimate business purposes or as required by law. 2. Limit use of and/or access to records, data applications, and/or systems containing confidential information to those persons who have a legitimate business purpose for such use and/or access. 3. Permit use of and/or access to Caris College's confidential information by only authorized individual(s) for legitimate business reasons. 4. Do not store confidential information on personally owned Portable Devices. 5. Do not manipulate or disregard security measures that have been put in place to protect confidential information, including, but not limited to, access controls, cameras and secure storage for card and device inventory, as well as tracking and monitoring of individuals' use of and/or access to confidential information. 6. Secure confidential information in a manner that is consistent with the ISP's rules for protecting information security of any files and other records containing confidential information. 7. Securely dispose of physical and electronic records containing confidential information at the earliest opportunity consistent with business needs and records retention requirements in the following manner: a. Physical documents containing confidential information are redacted, burned, pulverized, cross-cut shredded, or otherwise securely erased so that confidential information cannot practicably be read or reconstructed; and b. Electronic media and other non-physical media containing confidential information are destroyed or otherwise securely erased so that such information cannot be read or reconstructed. 8. Upon ceasing employment/contractual service with Caris College, (1) return all records, data applications and/or systems, in any form, including, but not limited to, information stored on laptops or other Portable Devices or media, and in files, records, and work papers, and (2) surrender all keys, identification cards, and all other means of using and/or accessing Caris College's premises and/or information. Any exception must be authorized in writing by the President / Chief Executive Officer.
Role	**External Risk Mitigation Responsibilities**
Institutional Management	1. Obtain acknowledgement, via the completion of the required online training course, that all personnel and POIs have received a copy of the ISP and will abide by its provisions. 2. Require that responsible parties at all Caris College sites work with the QI to establish exit processes which require personnel and POIs who cease employment with Caris College ("Separated Individuals") (1) return all

	records, data applications and/or systems, in any form, including, but not limited to, information stored on laptops or other portable devices or media, and in files, records, and work papers, and (2) surrender all keys, identification cards, and all other means of using and/or accessing Caris College's premises and/or information.
Management through enforcement of Administrative Regulations	1. Require that personnel and POIs immediately report any suspicious or unauthorized use of confidential information to the QI who coordinates with the IRT to appropriately respond. 2. Require that personnel and POIs who violate the ISP may be disciplined according to the severity of the violation, regardless of whether confidential information was accessed or used without authorization.
President/CEO	1. Require that all employment and consulting agreements contain provisions that (1) require all POIs to acknowledge, sign and comply with the provisions of the WISP, and (2) prohibit any nonconforming use of Confidential Information during or after employment. 2. Authorize in writing any and all exceptions to external risk mitigation responsibilities. 3. Seek legal advice as needed in connection with any and all aspects of WISP compliance.
Information Technology Consultant	1. At the direction of the appropriate manager, revoke separated individuals' physical, electronic, and remote electronic use of and/or access to confidential information.
Personnel and POIs	1. Prohibit removal of confidential information from the Caris College business premises (whether owned, leased, rented or otherwise utilized by Caris College) in electronic or written form absent (i) an approved, legitimate business need and (ii) use of reasonable security measures, as described in this ISP. 2. Encrypt or deliver by an alternative, more secure method all records and files containing confidential information that are transmitted wirelessly or across public networks. 3. Protect all passwords. Keep passwords in a location and format that are secure. 4. Contact the QI to ensure evaluation of all vendors, subcontractors and third-party products in advance of any work or purchase. 5. Require that all vendors, subcontractors and third-party products be evaluated in advance of any work or purchase. 6. Upon ceasing employment with Caris College, (1) return all records, data applications and/or systems, in any form, including, but not limited to, information stored on laptops or other portable devices or media, and in files, records, and work papers, and (2) surrender all keys, identification cards, and all other means of using and/or accessing Caris College's premises and/or information.

Definitions: As used in this administrative regulation, the following terms have the respective meanings set forth below:

FERPA: Family Educational Rights and Privacy Act; a federal law that protects the privacy of student education records. "Education records" are "those records, files, documents, and other materials which 1) contain information directly related to a student; and 2) are maintained by an educational institution." (20 U.S.C. § 1232g(a)(4)(A); 34 CFR § 99.3). FERPA applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

GLBA aka Financial Services Modernization Act of 1999: Gramm–Leach–Bliley Act; an Act that requires "financial institutions," including, but not limited to, colleges and universities, to protect the privacy of their customers, including information that customers provide to a financial institution that would not be available publicly ("personally identifiable financial information (PIFI)").13 Caris College, therefore, has a responsibility to secure the personal records of its students and employees. To ensure this protection, GLBA mandates that all financial institutions establish appropriate administrative, technical, and physical safeguards. GLBA also requires financial institutions to provide notice to customers about their privacy policies and practices, but institutions of higher education are generally exempt from this requirement, because they already do so under FERPA. Colleges and universities complying with FERPA are considered to be in compliance with GLBA.

HIPAA: Health Insurance Portability and Accountability Act of 1996; an Act to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Incident Response Team (IRT): The internal ad hoc team of professionals that is convened to provide incident handling services to Caris College during an ongoing information security event and to respond to an information security incident when the need arises.

Payment Card Industry Data Security Standard (PCI DSS): Payment Card Industry Data Security Standard; a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, automated teller machine (ATM), and point-of-sale (POS/ePOS) cards. "Payment card information" is any personally identifiable information associated with a cardholder, such as the cardholder's account number, account expiration date, name, address, or social security number. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered payment card information.

Personnel: All full-time, part-time and temporary employees and faculty who work for the Caris College organization.

POI: Person(s) of Interest; individuals such as the following who are not considered part of the Caris College workforce but who are still of interest to the organization:

Person of Interest Category	Definition
Consultant	Individuals who are hired to do specialized work for Caris College and are paid by outside sources
Agency temporary employee	Temporary agency employees who come to work for Caris College and are paid by the temporary agency

Retired employee	Retired employees who continue a relationship with Caris College are changed from Employee status to Person of Interest status
Call center or contract employee	Employees who provide support for some of our systems and are paid by the contracted company
Unpaid intern	An individual who is completing an internship at Caris College for credit in their degree program
Volunteer	An individual who is working at Caris College on a volunteer basis
Vendor	Members of organizations that provide services to Caris College employees and students
ESS Educational Services (e.g., hospitals providing clinical learning opportunities)	Members of organizations that have contractual relationships with Caris College for specialized programs

Portable Devices: Examples of portable devices include, but are not limited to, CDs, DVDs, eReaders, external hard drives, Google Glasses, laptops, memory sticks, smart phones, tablets, thumb drives, and USB drives.

Security Incident: The unauthorized access to and/or misappropriation of confidential information.

Confidential Information: Information that is so deemed under applicable law. Personally identifiable information, personally identifiable education records, individually identifiable health information, personally identifiable financial information and payment card information are examples of Confidential Information covered under the Arizona Revised Statutes (ARS), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm–Leach–Bliley Act (GLBA aka Financial Services Modernization Act of 1999) and Payment Card Industry Data Security Standard (PCI DSS), respectively.

Separated Individuals: Personnel and POIs who cease employment with Caris College.

Technology Resources: Caris College Administrative Regulation Technology Resource Standards provides the following examples of technology resources: Websites, applications (such as, but not limited to, Caris College's Populi Student Information Management System and Learning Management System), desktop and laptop systems, printers, central computing facilities, Caris College-wide or college-wide networks, local-area networks, telephones, facsimile machines, scanners, access to the Internet, electronic mail and similar electronic devices and information.

Reference(s):

Caris College Administrative Regulation Technology Resource Standards

Caris College Administrative Regulation Information Security Incident Response Plan

Caris College Administrative Regulation Identity Theft Red Flag and Security Incident Reporting

Contact(s):

Pursuant to Caris College Administrative Regulation Identity Theft Red Flag and Security Incident Reporting, anyone who notices that a Caris College technology resource(s) is currently being or may have been used in an inappropriate fashion should contact the QI via email at bkepley@cariscollege.edu.

Pursuant to Caris College Administrative Regulation Identity Theft Red Flag and Security Incident Reporting: (1) anyone, including, but not limited to, any Caris College personnel and POIs, who notices and/or suspects that Caris College confidential information may currently be or may have been exposed to someone without authorization should immediately contact the QI at bkepley@cariscollege.edu, who is designated as the exclusive recipient of reports of this nature. The Qualified Individual is responsible for obtaining details about the situation from the individual(s) and coordinating with the IRT to take any additional actions that the IRT deems necessary. Responsibilities of the IRT are described in Caris College Administrative Regulation Information Security Incident Response Plan.

Caris College, in consultation with legal counsel, is responsible for completing the analysis necessary to determine whether a breach has indeed happened. Deciding whether a breach of confidential information has happened is a complex technical and legal determination that involves detailed analysis. Neither Caris College personnel, POIs, nor students should postpone notification of the QI until a breach determination has been made. Instead, Caris College encourages anyone to report their hunch or suspicion, since Caris College counts on everyone to share the responsibility for keeping information secure.

Please email bkepley@cariscollege.edu with any questions and concerns about the Caris College administrative regulations.

Oversight

GLBA requires the College to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. In the course of business, the College may share covered data with third parties. Such activities may include collection activities, transmission of data or documents, destruction of documents or media, or other similar services.

The ISP will ensure that reasonable steps are taken to select and retain services providers that are capable of maintaining appropriate safeguards for the customer information at issue and by requiring service providers, by contract, to implement and maintain such safeguards.

The ISP's QI will identify service providers who have or will have access to covered data and will work with the Caris College legal staff and other offices as appropriate, to ensure that service provider contracts contain appropriate terms to protect the security of covered data. Contracts are reviewed to ensure the following language is included:

[Service Provider] agrees to implement and maintain a written comprehensive information security program containing administrative, technical and physical safeguards for the security and protection of customer information and further containing each of the elements set forth in § 314.4 of the Gramm Leach Bliley Standards for Safeguarding Customer Information (16 C.F.R. § 314). [Service Provider] further agrees to safeguard all customer information provided to it under this Agreement in accordance with its information security program and the Standards for Safeguarding Customer Information.

Evaluation/Testing

Caris College understands that ever-changing technology and constantly evolving risks require the review and adjustment of the Information Security Program. Evaluation will occur at least annually to ensure ongoing compliance with laws and regulations. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the QI, with the support of the designated Information Security Committee. Based on risk identification and assessment activities, the QI will assign specific responsibility for technical (IT), logical, physical, and administrative safeguards. Adjustments to the program are to reflect changes in technology, the sensitivity of student/customer data, and/or internal or external threats to information security.

A designated member of the ISP committee will be responsible for monitoring the FTC website as well as other qualified sites for changes/updates made to the GLBA Safeguards Rule.

Incident Response Plan

Caris College has an Incident Response Plan (IRP) in place, which outlines procedures for responding to actual or attempted unauthorized access to covered data. Specifically, in the event a security breach or an attack is discovered, the following steps will be taken:

1. Notifying all the affected parties immediately, in addition to the IT security team and the affected system's owner.
2. Creating a log that includes a list of the actions to be taken, with consistent updates provided to the involved parties by the Incident Response Team (IRT).
3. Identifying potential evidence, both conventional and electronic, considering that the condition of any electronic device *must not* be altered by either turning it on, off, or rebooting it until it is determined that it is safe to do so.
4. Gathering and collecting information from system monitors and other utilities that may aid in identifying the problems and the potential threats that caused them.
5. Regaining control of the system, e.g., network disconnection, process termination, system shutdown, or other actions to prevent further compromise of protected information.
6. Analyzing the incident; its type, impact on the College, potential cost to the College (in terms of time, money, etc.)
7. Applying corrections, if needed, to the ISP based on the conducted analysis.
8. Verifying the system integrity.
9. Restoring service completely once Step 8 has been verified.
10. Creating an incident report by the IRT which includes the details related to the incident including 1) data and time; 2) description; 3) list of compromised data; 4) identifiable risks; 5) corrective actions; 6) estimated costs of the corrective actions; and 7) personnel responsible for the incident.

The details of the IRP are available upon request from the College's Qualified Individual (QI).

The plan will be regularly updated to account for any new, unexpected threats in light of the growth of cutting-edge technology around us. Training provided to employees will also account for these new threats and will be constantly updated, with the aim of cultivating in the employees at the College that they are the most vulnerable and the most valuable asset to any type of attack or breach.

Reporting

The ISP Committee will evaluate and adjust the program based on the risk identification and assessment activities undertaken pursuant to the program, as well as any material changes to the College's operations, business arrangements, or other circumstances that may have a material impact on the program.

Written reports will be provided to the board members and those positions listed below periodically (at least annually) regarding all material matters relating to the Information Security Program.

- President
- Assistant Campus Director

- Director of Academic Operations
- Directors of Financial Aid
- Program Directors
- Internal Auditing

Caris College recognizes the significance of strong practices as it pertains to information security. To that effect, administrators will manage the review and execution of the institution's ISP. This will be an ongoing process projected to continuously strengthen security/protection measures in the safeguarding of confidential data.

[1] Confidential Information is information that is so deemed under applicable law. Personally identifiable information, personally identifiable education records, individually identifiable health information, personally identifiable financial information and payment card information are examples of Confidential Information covered under the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm–Leach–Bliley Act (GLBA aka Financial Services Modernization Act of 1999) and Payment Card Industry Data Security Standard (PCI DSS), respectively.

[5] The ISP will be reviewed and adjusted, where necessary, to maintain compliance with all applicable regulations, laws and contractual obligations and to gain increasing insight into (1) reasonably foreseeable internal and external risks to the security and confidentiality of any electronic, paper, or other records containing Caris College Confidential Information; (2) the likelihood and potential damage to Caris College from such threats; (3) the sufficiency of existing Caris College administrative regulations, procedures, information systems, and other safeguards in place to control risks to information security at MQC, and (4) methods for regularly monitoring and strengthening the effectiveness of those safeguards.

[6] All communications concerning information security and privacy must be approved by the President and Designated ISP committee members prior to publication.

[7] New Personnel and POIs must complete training within thirty (30) days of the start of their employment/contractual service at Caris College.

[8] To the extent relevant, this responsibility also applies to all Caris College students.

[9] This responsibility applies to all individuals granted use of and/or access to Caris College online technology resources.

[10] Any exception must be authorized in writing by the President.