Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, requires financial institutions that offer consumers financial products or services to explain their information-sharing practices to their customers and to safeguard sensitive customer data.

Because Palo Verde Community College District (PVCCD) engages in financial activities, it is considered by the Federal Trade Commission (FTC) to be a financial institution and is therefore required to be compliant with GLBA.

GLBA requirements

GLBA dictates several specific requirements regarding the privacy of customer financial information. These are codified in three rules:

1. Pretexting Rule

The Pretexting Rule is designed to counter identity theft.

To comply, PVCCD must have mechanisms in place to detect and mitigate unauthorized access to personal, non-public information (such as impersonating a student to request private information by phone, email, or other media).

2. Privacy Rule

The Privacy Rule is designed to govern the collection and disclosure of customers' personal financial information by financial institutions.

3. Safeguards Rule

The Safeguards Rule is designed to ensure the administrative, technical, and physical safeguarding of personal, non-public customer information.

The Safeguards Rule requires PVCCD to develop, implement, and maintain a comprehensive Information Security Program containing administrative, technical, and physical safeguards that are appropriate for the size, complexity, and nature of its activities, in order to:

- Ensure the security and confidentiality of customer records and information.
- Protect against any anticipated threats or hazards to the security or integrity of such records.

- Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Under GLBA, it is the obligation of PVCCD to establish appropriate standards for areas under its jurisdiction relating to administrative, technical, and physical safeguards for customer financial information or covered data.

(Back to top of page)

PVCCD compliance

1. Pretexting Rule

PVCCD supports:

- GLBA Pretexting Rule
- Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act) of 2003

To meet GLBA standards in this regard, PVCCD must:

a. Educate employees to recognize social engineering attacks
   The PVCCD IT Department actively promotes social engineering education for students, faculty, and staff.

    - IT Department has a prescribed method of engagement supporting victims of identity theft, including federal pamphlets and instructional materials.
    - Since 2019, PVCCD has mandatory cybersecurity training for all employees. Information Technology (IT) has conducted district-wide programs during October in support of National Cyber Security Awareness Month.
    - IT has made available several educational videos on various topics from "phishing" to "what to do if your identity has been stolen" that are posted on the PVCCD website.
    - The InfoSec and Client Services teams actively engage users in direct education when dealing with tickets and incidents.
    - The Service Desk is trained to answer general queries regarding information security and identity theft.

2. Privacy Rule

PVCCD is considered in compliance with the Privacy Rule because we are in compliance with the Family Educational Rights and Privacy Act (FERPA).

3. Safeguards Rule

Details on PVCCD's actions to comply with the Safeguards Rule can be found on the engaging with the Safeguards Rule page.

(Back to top of page)

Engaging with the Safeguards Rule

PVCCD's approach to satisfying GLBA requirements related to the Safeguards Rule is structured around addressing the following:

1. Defining the program's scope.

PVCCD places the highest value on its customer's information. We understand and accept our responsibility as custodians of their data. We respect and protect the privacy of our students, faculty, staff, and other third parties. And we value the relationships and sense of security we maintain with our customers.

For the purpose of this program, "customer information" is defined as any record containing nonpublic personal information about a customer of the college, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the college or its affiliates.

What is covered "nonpublic personal information"?

In this case, nonpublic personal information means personally identifiable financial information about a student or other third party, where such information is obtained in connection with the provision of a financial service or product by PVCCD, and that is maintained by PVCCD or on PVCCD's behalf.

Nonpublic personal information means:

- Information that a student or other third party provides in order to obtain a financial service or product from the college;
- Information about a student or other third party resulting from any transaction with the college involving a financial service or product; or
- Information otherwise obtained about a student or other third party in connection with providing a financial service or product to that person.

For example, nonpublic personal information includes bank and credit card numbers, income and credit histories; as well as names, addresses, and Social Security numbers associated with financial information.

Why is PVCCD engaging with GLBA?

An Institute of Higher Education, like PVCCD, that engages in financial activities (e.g. processing student loans) is considered by the Federal Trade Commission (FTC) to be a financial institution and is therefore required to be compliant with GLBA.

In 2015, compliance with the GLBA Safeguards Rule, 16 CFR 314.4 (b), was included in Title IV Program Participation Agreement by Department of Education. This directly tied PVCCD's ability to process student financial aid to GLBA.

The Safeguards Rule requires covered entities to consider risks in each relevant area of their operations, including:

- Employee training and management
- Information systems, including network and software design, as well as information processing, storage, transmission, and disposal, and
- Detecting, preventing, and responding to attacks, intrusions, or other systems failures

In 2015 and 2016 the Dept. of Education sent "Dear Colleague" letters to PVCCD urging compliance. In 2017 and 2018, the Dept. of Education's Office of Federal Student Aid drafted federal single audit guidance. It is anticipated that the federal single audit guidance will become final within the coming years.

How is PVCCD engaging with GLBA?

PVCCD's Information Security Program (ISP) has been developed to ensure and protect our customers' covered nonpublic personal information, as well as PVCCD institutional data. This includes hard copy (paper), electronic, or other forms of records; data; systems; services; and infrastructure components which are handled or maintained by or on behalf of the college or its affiliates.

In accordance with GLBA Safeguards Rule requirements and regulations issued by the Federal Trade Commission pursuant to that rule, PVCCD's ISP encompasses the following objectives:

1. Ensure the security and confidentiality of our customers' nonpublic personal information (e.g., names, addresses, Social Security numbers, etc.).
2. Protect the security and integrity of customer and institutional information against anticipated hazards or threats.
3. Protect customer and institutional information from unauthorized access or use, which could result in substantial harm or inconvenience.

In order to maintain and deliver these objectives, PVCCD utilizes a holistic approach with defined goals, which include:

1. Designating a team of employees to implement, coordinate, and manage information security.
2. Establishing routines for conducting risk assessments of systems and services, both internal and external, that could potentially lead to unauthorized disclosure or misuse of confidential information.
3. Establishing, coordinating, and managing safeguards to mitigate identified risks.
4. Requiring third-party service providers to implement and maintain established confidentiality protocols.
5. Periodically evaluating and modifying the ISP to ensure continuing protection of confidential information.

2. Implementing an Information Security Program

The ISP is designed to protect the confidentiality, integrity, and availability (or "CIA," the guiding principle of information security management) of PVCCD's information assets – data, systems, services, and infrastructure components – and seeks to protect any record containing customer information (see Appendix A).

The goals for the ISP are as follows:

1. Assure regulatory compliance with federal, state, and local law across all PVCCD departments.
2. Limit access to customer information to employees who have a business need to see it.
3. Ensure the security and confidentiality of customer records.
4. Safeguard and prevent unauthorized access to personally identifiable financial data.
5. Align with existing PVCCD policies, standards, guidelines, and procedures.
6. Ensure appropriate employee training and management.
7. Ensure information systems security best practices.
8. Detect, prevent, and remediate attacks, intrusions, or other information security risks.

3. Designating employee

PVCCD's Director of Information Technology is the designated ISP Coordinator for PVCCD.

4. Performing risk assessments

The ISP Coordinator assists department heads or managers to ensure that GLBA-related risks are included in the overall College-wide Risk Management Program.

Additionally, PVCCD intends, as part of the ISP, to undertake a risk assessment to identify and assess reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromises of such information. At a minimum, the risk assessment will include consideration of risks in each relevant area of PVCCD operations, including:

- Employee training and management
  Consider the effectiveness of current employee training and management procedures relating to the access and use of covered information.
- Information systems, information processing, and disposal
  Assess the risks to covered information associated with information systems, as well as information processing, storage, transmission, and disposal.
- Detecting, preventing, and responding to attacks and system failures
  Consider procedures for and methods of detecting, preventing, and responding to attacks, intrusions, or other system failures.
- Designing and implementing safeguards
  Safeguards will be designed and implemented in order to control the risks identified through the GLBA risk assessment. The ISP Coordinator, in collaboration with appropriate institutional representatives, will monitor the effectiveness of the safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures. It is the College's intent to use the National Institute of Standards and Technology (NIST) SP 800-171 Rev. 2 as a model to assess and address gaps in safeguards, as appropriate.

Focus areas

When identifying areas of focus, look for changes since the last review (refer to Appendix B). The Federal Trade Commission provides general guidance for complying with the Safeguards Rule.

5. Employee training and management

PVCCD safeguards for security will include management and training of those individuals with authorized access to covered data. This includes training in FERPA, PVCCD's Information Security and Acceptable Use policies, procedures and practices relating to access to and use of customer information, and specific training in accordance with GLBA accountability.

- Employees with access to covered data must abide by PVCCD policies and procedures governing covered data, as well as any additional practices or procedures established by their department heads or directors.
- The ISP Coordinator will designate individuals who have the responsibility and authority for information technology resources, establish and disseminate enforceable rules regarding access to and acceptable use of Information Technology resources, establish reasonable security policies and measures to protect data and systems, monitor and manage system resource usage, and investigate problems and alleged violations of covered information. The ISP Coordinator will refer violations or non-compliance to

appropriate offices such as the ISOC, legal counsel, President or Board of Directors, Internal Auditor, or Human Resources for resolution or disciplinary action.

Curriculum

It is essential that every employee who has access to or uses covered data have at least annual training on GLBA compliance. PVCCD is in the process of developing GLBA training materials, which will include:

- Covered data and data ownership
- Confidentiality, integrity, and availability
- Physical security
- Access controls
- Encryption
- Social engineering
- Policies
- Fraud

6. Overseeing service providers

Consistent with the provisions of GLBA, PVCCD takes reasonable steps to select and retain service providers that maintain appropriate safeguards for covered data and information.

For technology products and services, the IT purchasing team works closely with the college purchasing and contracts teams to ensure that all IT purchases and contracts are processed in accordance with applicable Federal and State laws and PVCCD purchasing standards.

New vendor relationships are subject to information security, cyber insurance coverage, and accessibility reviews. Specifically, such reviews are geared toward ensuring methods for selecting and retaining service providers that are capable of maintaining appropriate safeguards for covered information.

In the course of business, PVCCD may appropriately share covered data with third parties. Such activities may include collection of data, transmission of documents, transfers of funds, destruction of documents or equipment, or other similar services. The ISP will ensure that reasonable steps, including consultation with legal counsel, are taken to select and retain service providers that are capable of maintaining appropriate safeguards for customer information and requiring service providers by contract to implement and maintain such safeguards.

7. Evaluating and adjusting the ISP

The ISP is maintained based on the principles of continual risk management. Risks change with time, as business and the environment changes. As a result, strong controls will degrade over time and are subject to eventual failure. In addition, countermeasures may introduce new risks.

The overall information security program is periodically evaluated and adjusted to reflect changing college business, measurements of program effectiveness, and lessons learned from the implementation of security safeguards.

8. Program governance

Enforcement

Violation of the ISP may result in disciplinary action, up to and including termination of employment.

Exceptions

Any exceptions to the GLBA ISP must be approved by the College President upon the recommendation of the ISP Coordinator.

Resources

- Information Security Policy
- IT Service Desk
- IT Department

Program questions

Questions regarding the GLBA Program or regarding information security may be emailed to: cio@paloverde.edu

Approval

Approved by Eric Egan, Director of Information Technology Officer, October 5th, 2020

Program review

This program will be reviewed and updated as needed, at least annually, based on the recommendations of the ISP Coordinator.

Personal, non-public information

There are several terms used to identify similar sets of protected data.

PVCCD policy uses the term "controlled sensitive data" which is equivalent to, but more encompassing than, "personal, non-public information".

Additionally, Personally Identifiable Information (PII) is a critical subset of protected data, but does not cover all categories of data protected under GLBA.

GLBA regulation also uses the terms "covered data" and "sensitive customer data".

More details regarding the use and meaning of these terms can be found in Appendix A.

(Back to top of page)

Appendix A: Data classifications

PVCCD data

PVCCD data is any data related to PVCCD operations that is

1. Stored on PVCCD information technology systems
2. Physically recorded and stored on PVCCD premises
3. Maintained by PVCCD faculty, staff, or students
4. Related to institutional processes on or off campus

Critical versus non-critical

PVCCD Data is either critical or non-critical:

Non-critical data is information considered public and non-confidential in nature. Non-critical data is not subject to protection or data handling procedures.

Critical data is information considered valuable to some degree to PVCCD. Classification of critical data varies based on the context and use case with respect to the value of the information, the degree of protection required, and the degree of damage that unauthorized disclosure would cause. Critical information is not releasable on demand without due process.

Some examples of critical data are:

- Personally Identifiable Information (PII)
- Financial account numbers
- Passwords
- Information that may have a derogative impact on PVCCD, staff or students of PVCCD
- Internal communications that may have a derogative impact on PVCCD operations if sent to someone without a need to know
- Health-related information
- Any information deemed confidential, restricted or academically sensitive

Critical data classifications

The following are the most common terms and classifications of critical data in use at PVCCD:

Personally identifiable information (PII)

A commonly used security industry term that describes any data that could potentially identify a specific individual. PII is any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data. PII may be a single unit of data (e.g. a social security number) or may result from the combining of related pieces of information (e.g. a user name and password).

GLBA covered information

PVCCD is required to protect covered customer data in accordance with the Gramm Leach Bliley Act (GLBA). GLBA defines covered customer information as any record containing nonpublic personal information or personally identifiable financial information about a customer of PVCCD – whether in paper, electronic, or other form – that is handled or maintained by or on behalf of PVCCD or its affiliates.

GLBA nonpublic personal information

Nonpublic personal information is GLBA's terminology for customer data covered by the regulation. It includes:

- Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available
- Any information a student or other third party provides in order to obtain a financial service from PVCCD
- Any information about a student or other third party resulting from any transaction with PVCCD involving a financial service
- Any information otherwise obtained about a student or other third party in connection with providing a financial service to that person

Examples of nonpublic personal information include (but are not limited to):

- Social Security number
- Credit card number
- Account numbers
- Account balances
- Any financial transactions
- Tax return information
- Driver's license number
- Date or location of birth

Examples of services or activities that PVCCD may offer, which result in the creation of nonpublic personal information, could include (but are not limited to):

- Student (or other) loans, including receiving application information and the making or servicing of such loans
- Credit counseling services
- Collection of delinquent loans and accounts
- Check cashing services
- Obtaining information from a consumer report

Protected data

Information considered valuable to PVCCD but not requiring confidentiality controls. Unclassified information may have additional departmental controls on the handling, collection, processing, and/or distribution. Examples of this would include destruction or storage dates/instructions, rare historical documents, copyrighted materials, and special instructions such as conditional access provisions.

Academic data

A classification of critical information controlled for academic purposes to maintain academic freedom. This does not include student personal identification.

Academic data deals with faculty lesson and testing content. This includes but is not restricted to test banks, quizzes, sequential lesson material, answer keys, or research conducted by faculty affiliated with PVCCD or research conducted on the premises with other institutions. It also can include information regarding academic thesis research by faculty.

Academic information disclosure can degrade the integrity of grades, the reputation of PVCCD, the student body, and faculty as a whole. It can also cause enormous financial losses and penalties due to the illicit exploitation of research.

Internal data

A classification of critical information considered medium to high risk, because the exposure of this information can cause serious harm to PVCCD. Information in this category is largely proprietary and operational in nature. This includes information about PVCCD-related activities. Examples include detailed information about some information technology infrastructure, PVCCD buildings, security procedures, activities or events, information about future PVCCD development plans, and grant information.

Confidential data

A classification of critical information considered high risk, either because the exposure of this information can cause tremendous harm to an individual or PVCCD or because the information is specifically protected under law or contract (e.g. HIPAA, FERPA, GLBA, and PCI).This includes information that can be linked, directly or indirectly, to individual people. Social security numbers, credit card numbers, financial information, personally identifiable medical information, personal addresses, and personally identifiable academic information fall into this category.

Data in these categories will require varying security measures appropriate to the degree to which the loss or corruption of the data would impair the business functions of the PVCCD, result in financial loss, or violate law, policy or PVCCD contracts.

Controlled sensitive data

An encompassing definition used in PVCCD's Information Security policies that references all confidential and private information governed by those policies. This includes data classified as PII, regulated data (PHI, HIPAA, FERPA, GLBA, etc.), protected, academic, internal or confidential data. In simple terms, any critical personal or sensitive information for which PVCCD is liable if publicly disclosed.

(Back to top of page)

Appendix B: Focus areas

Following are some areas for consideration when analyzing the effectiveness of safeguards (this is not intended to be a comprehensive list).

Response history

- Incident response documentation and audits

Enterprise operations

- Management, organization, business strategy, or operational procedures
- Information technology environment
- Changes in key service providers

Departmental operations

- Key operational metrics (system availability, etc.)
- Operating environment aligned to business needs
- Adequacy of operational technology

Risk management

- Risk ledger
- Controls aligned with identified risks
- Coordination of operations risk

Technical documentation

- Systems diagrams and topologies describing the interrelationship between architectural components
- Documentation of processes and technical controls

Personnel management

- Appropriate organizational structure
- Background checks for employees
- Sufficient segregation and rotation of duties
- Retention policies and procedures
- Separation/termination policies and controls

Backup and recovery

- Enterprise data storage methodologies
- Data backup strategies
- Data and program file asset inventory
- Back-up procedures that meet recovery time objectives
- Off-site storage facility and inventory management procedures meet generally accepted standards
- Adequate environmental monitoring and controls

Network and telecommunications

- Architecture and process alignment with strategic goals
- Operations monitoring for downtime, throughput, usage, and capacity utilization, etc.
- Availability, speed, bandwidth/capacity, resiliency and continuity
- Adequate security controls

Data at rest

- Identity and access management
- Encryption
- Database administration
- Network controls

Data in transit

- Encryption
- Least Access
- Monitoring/exfiltration

Imaging systems

- System data flow, topology and usage patterns
- Confidentiality, availability, integrity

- Destruction of source documents (e.g., shredded)
- Compliance with regulations and other standards, including legal counsel review
- Business continuity planning
- Segregation of duties and least access

End-point management

- Identity and access management
- Vulnerabilities and patching
- Images and customized configurations
- High value workstations
- Laptops and mobile devices

Incident and problem management

- Identifying, analyzing, and resolving issues and events
- Controlling data modifications or corruption
- Forensic training and awareness

Corrective action and communication

- Document effectiveness of controls
- Violations of law, rulings, regulations
- Significant issues warranting inclusion as matters requiring Board of Directors' attention
- Noncompliance with supervisory guidance

(Back to top of page)

Appendix C: Data management roles

Data Originator

Data Originators have Original Classification Authority (OCA) to set the initial classification level of a piece of information they create in whole or in part. Only Data Trustees have the authority to revise a classification level.

Note: Data Originators do not have the authority to downgrade confidential information, since the protections required are usually the result of legal or contractual requirements.

Data Owner

The department, division, or other administrative unit manager that is directly responsible for the management and maintenance of the data stored on computer storage device or media.

Data Steward

Data Stewards are PVCCD staff having direct operational-level responsibility for information management. They are usually department managers or designated system analysts.

Data Stewards are responsible for providing a secure infrastructure in support of the data – including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized by data trustees or their designees, and implementing and administering controls over the information.

Data Trustee

Data Trustees are senior PVCCD officials (or their designees) who have planning and high-level responsibility for data within their functional areas and management responsibilities for defined segments of institutional data.

Data Trustees are ultimately responsible for the accuracy and protection of data in their areas. Responsibilities include assigning data stewards, participating in establishing standards, practices, and accountability.

Data User

Data users are individuals who need and use PVCCD data as part of their assigned duties or in fulfillment of assigned roles or functions within the PVCCD community. Individuals who are given access to sensitive data have a special position of trust and are responsible for protecting the security and integrity of those data and should exercise due care in using the institution's accessing information systems and to protect files from unauthorized use, disclosure, alteration, or destruction. Each user is responsible for security, privacy, and control of their own data.