Information Security Program & Compliance Policy

Document Name:	Information Security Program & Policy
Document ID:	POL-01
Tags:	Information Security, Risk, Responsibilities, Continuous Monitoring, Asset Management, Encryption, Access and Authentication, Third-party Risk, Vulnerability Management, Awareness and Training

APPROVALS

CIO, Institutional Risk Management:	XX XX, 2024
Executive Management:	
Included NIST 800-53 Rev. 5 Controls:	CA-2, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, ID.AM-1, IA-2,AD.SC-3,PR.AT, PM-14, PS-1, RA-3
Included CIS 18 Version 8 Safeguards:	1.1, 1.2, 3.1, 6.5, 7.1,8.1, 13.1, 14.1, 15.1, 17.1, 18.1

CONTENTS

1. PURPOSE

The Information Security Program and Compliance Policy is designed to protect the college's data and ensure it meets GLBA requirements. Its main objectives are to prevent unauthorized access to sensitive information, maintain the accuracy and integrity of data, and ensure its availability when needed. The program helps in identifying potential security threats and vulnerabilities, and it outlines controls required to protect information assets. Additionally, it ensures that college employees receive proper training to understand the policies and practices.

2. AUTHORITY

Centenary College of Louisiana

3. SCOPE

This policy encompasses all systems, automated and manual, for which Centenary College has administrative responsibility, including systems managed or hosted by third parties on behalf of the entity. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

4. POLICY

4.1 General

Centenary College has adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework version 2.0 as the program framework, along with the Center for Internet Security Controls Version 8 as the control framework. Additionally, other industry best practices and standards have been incorporated to guide information security practices. These established standards will ensure compliance with the Gramm-Leach-Bliley Act (GLBA).

Information security requires both an information risk management function and an information technology security function. Risk management decisions must be made based on both functions.

The College's Cabinet approves this policy and any subsequent changes. The Chief Information Officer (CIO) is tasked with managing this policy and the associated maintenance activities, which encompass reviews and revisions.

Centenary College has designated the CIO to be responsible for assuring that risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed as an enterprise with regard to the overall strategic goals and objectives of carrying out its core missions and business functions; and the management of information assets and information system-related security risks is consistent, reflects the risk tolerance, and is considered along with other types of risks, to ensure mission/business success. The CIO will make these decisions in consultation with the Vice President for Finance and Administration & CFO.

Centenary College has designated the IT team to be responsible for the technical information security function.

5. RESPONSIBILITIES

Cabinet is responsible for:

- Evaluating and accepting risk recommended by the CIO on behalf of Centenary College;
- Escalating and reporting cybersecurity risk and cybersecurity risk decisions to Centenary College board;
- Supporting the consistent implementation of information security policies and standards;
- Ensuring the provision of adequate resources for the implementation of information security controls that conform to NIST and GLBA standards.
- Participating in the response to security incidents;
- Complying with notification requirements in the event of a breach of private information;
- Adhering to specific legal and regulatory requirements related to information security;
- Communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.

Vice President for Finance and Administration & CFO:

- Oversee the process for determining information classification and categorization, based on industry recommended practices, organization directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information;
- Oversee the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization;
- Oversee who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data;

- Participate in the response to security incidents;
- Complying with notification requirements in the event of a breach of private information;
- Adhering to specific legal and regulatory requirements related to information security;
- Communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.

The CIO/designated security representative:

- Enforce Information security and NIST, GLBA compliance
- Leads, supervises, directs the IT Management Team
- Develop, design, recommend, and implement the process for determining information classification and categorization, based on industry recommended practices, organization directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information;
- Develop, design, recommend, and implement the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization;
- Determine who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data;
- Promote awareness of information security best practices through the regular dissemination of materials
- Identify information security responsibilities and goals and integrating them into relevant processes;
- Maintain familiarity with business functions and requirements;
- Communicate and implement legal and regulatory requirements to Centenary College
- Maintain an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education (CPE) credits directly related to information security;
- Assess compliance with information security policies and legal and regulatory information security requirements;
- Evaluating and understand information security risks and how to appropriately manage those risks;
- Develop, design, recommend and implement the security program and strategy, including measures of effectiveness;
- Establish and maintain enterprise information security policy and standards;
- Represent and assure security architecture considerations are addressed;
- Advise and approve security issues related to procurement of products and services;
- Escalate security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;
- Disseminate threat information to appropriate parties;
- Participate in the response to potential security incidents;
- Participate in the development of enterprise policies and standards that considers Centenary College's needs; and
- Review monitoring reports for anomalies or trends for all systems.
- Lead incident response and disaster recovery exercises
- Oversee access review processes to ensure completion by applicable data owners.

- Monitor activities by domain admins and other privileged users on all systems and critical applications.

IT Management Team is responsible for:

- Supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners;
- Providing resources needed to maintain a level of information security control consistent with this policy;
- Manage and assess third-party relationships, processes and interactions with Centenary College networks
- Identifying and implementing all processes, policies and controls relative to security requirements defined by the business and this policy;
- Implementing the proper controls for information owned based on the classification designations;
- Providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);
- Fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting and implementing appropriate and cost-effective security controls and procedures; and
- Implementing business continuity and disaster recovery plans.
- Providing in-house expertise as security consultants as needed;
- Advising on secure system engineering;
- Providing incident response coordination and expertise;
- Monitoring networks for anomalies;
- Monitoring external sources for indications of data breaches, defacements, etc.
- Maintaining ongoing contact with security groups/associations and relevant authorities;
- Providing timely notification of current threats and vulnerabilities; and
- Providing awareness materials and training resources.
- Completing ongoing training relevant to the position held, and level of access maintained.

The workforce is responsible for:

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted;
- Protecting information and resources from unauthorized use or disclosure;
- Protecting personal, private, sensitive information from unauthorized use or disclosure;
- Abiding by *Computer Use Policy*
- Reporting suspected information security incidents or weaknesses to the appropriate manager and CIO/designated security representative.

5.1 Separation of Duties

To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.

Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision.

The audit and approval of security controls must always remain independent and segregated from the implementation of security controls.

6. RISK MANAGEMENT

Risk management is a critical component of any information security program and is also a requirement of GLBA. It helps ensure that any risk to confidentiality, integrity, and availability is identified, analyzed, and maintained at acceptable levels. Risk assessments allow management to prioritize and focus on areas that pose the greatest impact to critical and sensitive information assets. This provides the foundation for informed decision-making regarding information security.

Information security risk management considers vulnerabilities, threat sources, and security controls that are planned or in place. These inputs are used to determine the resulting level of risk posed to information, systems, processes, and individuals that support business functions.

It should be noted that Centenary College can never completely eliminate risk but can take steps to manage risk.

Routine risk assessments are needed to identify risk and ensure appropriate controls.

- Any system or process that supports business functions must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development life cycle.
- Information security risk assessments are required for new projects, implementations of new technologies, significant changes to the operating environment, or in response to the discovery of a significant vulnerability.
- Entities are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.
- Risk assessment results, and the decisions made based on these results, must be documented.

6.1 Asses Risk

Risk is assessed by determining the threats and vulnerabilities to these assets, identifying the potential impact of each vulnerability being exploited, and determining the likelihood of occurrence. A list of potential threats and vulnerabilities needs to be developed and may come from preexisting resources.

The following risk model will be used to assess risk:

Impact:

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Likelihood:

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

Risk:

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	**Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

It is important to note that the risk assessment process is comprehensive by intention, to assure the confidentiality, integrity, and availability of information on all systems, applications, and proper documentation of security related controls and considerations.

The scope of the risk assessment should be commensurate with the classification (information sensitivity and system criticality) of the system/process and the risks this system/process introduces into the overall environment.

While risk management and related assessment activities can take many forms (e.g., formal risk assessment, audits, security reviews, configuration analysis, vulnerability scanning and testing), all are aimed at the same goal - identifying and acting on risk to improve overall security posture. Assessment activities and risk identification may be performed by any of the parties listed in the responsibilities section above.

6.2 Respond to Risk

Once risk has been assessed, the CIO will advise management on the appropriate course of action for all identified Very High, and High. Management options for treatment include:

- Risk Acceptance – This is a documented decision not to act on a given risk at a given time and place. It is not negligence or “inaction” and can be appropriate if the risk falls within the risk tolerance level. Alternate risk mitigation recommendations must be thoroughly evaluated prior to risk acceptance.
- Risk Avoidance – These are specific actions taken to eliminate the activities or technologies that are the basis for the risk. This is appropriate when the identified risk exceeds the risk tolerance, even after controls have been applied (i.e., residual risk).

- Risk Mitigation/Reduction – These are specific actions taken to eliminate or reduce risk to an acceptable level. This is the most common approach and is appropriate where controls can reduce the identified risk.
- Risk Transfer/Sharing – These are specific actions taken to shift responsibility for the risk, in whole or in part, to a third party. This may be appropriate when it is more cost effective to transfer the risk, or when a third party is better suited to manage the risk.

On a discretionary basis, the CIO will communicate risk treatment decisions to Centenary College Executive Leadership and the IT Management team.

6.3 Monitor Risk

The purpose of monitoring risk is to:

- Verify that planned risk response measures are implemented and information security requirements derived from organization mission/business functions, federal/state legislation, directives, regulations, policies and standards, guidelines, and compliance are satisfied.
- Determine the ongoing effectiveness of risk response measures following implementation.
- Identify risk-impacting changes to organizational information systems and the environments in which the systems operate.

The CIO must monitor the effectiveness of its risk response measures, by verifying that the controls put in place are implemented correctly and operating as intended. This must occur annually, at a minimum. In addition, the entity must have a process to alert it of significant changes in the factors it uses to assess its risk (e.g., assets, threats, controls, regulations, policies, risk tolerance). These changes may indicate a new assessment is needed.

7. CONTINUOUS MONITORING

Audit records and logs are to be monitored under a continuous monitoring strategy to ensure the ongoing assessment of controls and to support incident management practices. Information must also be received on an ongoing basis from information system security alerts, advisories, and directives

Continuous monitoring efforts must be used to detect:

- Attacks and indicators of potential attacks.
- Unauthorized local, network, and remote connections.
- Tracking the use of software and associated documentation protected by quantity licenses to control copying and distribution.
- GLBA 314.4 C.8 states "*Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users*." While the bullet above somewhat addresses it, it does not adequately address user activity

The level of information system monitoring activity should be increased whenever there is an indication of increased risk to operations and assets, individuals, other organizations, or based on law enforcement information, intelligence information, or other credible sources of information.

Information system monitoring activities must be conducted in accordance with applicable state and federal laws, directives, policies, or regulations.

Information system monitoring information must only be provided to authorized personnel or business units as needed.

Effective continuous monitoring includes status monitoring and reporting of metrics on a frequency basis to Centenary College Executive Leadership and the Enterprise Risk Management team.

8. ASSET MANAGEMENT

All Information Technology (IT) resources and information systems are acquired and tracked to meet the information systems mission and business objectives. All IT resources and information systems must be assigned to a designated business unit or individual.

Entities are required to maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible.

Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

9. ENCRYPTION

Encryption of customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access, is required.

This includes storage on computers, laptops, servers, portable devices, and in transmissions such as emails and for wireless connections.

The use of Secure Sockets Layer (SSL) should be utilized when accessing or transmitting customer information to or from any website.

Transmission of customer information via other methods should use secure and encrypted mechanisms to safeguard and protect customer information. FIPS 140-2 compliant or AES-256 equivalent encryption MUST be used.

The file, document, or folder containing customer information should be encrypted before transmission.

Users should not send customer information via email or messaging systems if encryption has not been implemented.

The following secure methods may be used:

- An approved secure file transfer system
- An authorized encrypted mobile media device
- An approved secure email solution

If necessary, contact IT management to determine what type of secure methods can be used.

Users should not access customer information when using public non-encrypted wireless networks.

10. DATA CLASSIFICATION AND HANDLING

- All information, which is created, acquired or used in support of business activities, must only be used for its intended business purpose.
- All information assets must have an information owner established within the lines of business.

- Information must be properly managed from its creation, through authorized use, to proper disposal.
- All information must be classified on an ongoing basis based on its confidentiality, integrity and availability characteristics.
- An information asset must be classified based on the highest level necessitated by its individual data elements.
- If the entity is unable to determine the confidentiality classification of information or the information is personal identifying information (PII) the information must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.
- Merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted.
- All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.
- The entity must communicate the requirements for secure handling of information to its workforce.
- A written or electronic inventory of all information assets must be maintained.
- Content made available to the general public must be reviewed according to a process that will be defined and approved by the College. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.
- PII must not be made available without appropriate safeguards approved by the College.
- For non-public information to be released outside the entity or shared between other entities, a process must be established that, at a minimum:
    - evaluates and documents the sensitivity of the information to be released or shared;
    - identifies the responsibilities of each party for protecting the information;
    - defines the minimum controls required to transmit and use the information;
    - records the measures that each party has in place to protect the information;
    - defines a method for compliance measurement;
    - provides a signoff procedure for each party to accept responsibilities; and
    - establishes a schedule and procedure for reviewing the controls.

11. ACCESS AND AUTHENTICATION

Access controls on information systems, including controls to authenticate and permit access only to authorized individuals to ensure that all users have appropriate access to customer information and to prevent those users who do not have authorized access from obtaining access to customer information.

Access to information systems will be granted as a result of a documented request from the user's supervisor and will be based on a minimum needs basis, i.e. users will be provided access to perform their job responsibilities but no more than. When determining the appropriate level of access to award a user, in addition to applying the principle of least privilege, additional controls including dual control and segregation of duties will be considered.

To gain access to Centenary College systems, the user must be provided a unique username and password. Users are strictly forbidden from sharing their passwords.

All passwords will be alphanumeric, at least 8 characters in length, and composed of a combination of uppercase and lowercase letters, numbers, and symbols.

Privileged user accounts credentials will be held to a higher standard than user level accounts and require the approval of the CIO before creation. Privileged user accounts will only be established for systems that individual maintains or requires access to. Privileged accounts must also be granted on a minimum needs basis.

Password reuse is not permitted.

Centenary College does not maintain a master list of passwords. the employee signs-on.

In addition to requiring a username and password, Centenary College will also utilize Multi Factor Authentication (MFA) to protect access to web-based applications containing customer information and other high-risk information systems.

User account must be locked after three unsuccessful tries for login.

User accounts for terminated employees must be disabled no later than three business days following the employee's last day of employment. User accounts for termination employees must be deleted no later than sixty business days following the employee's last day of employment.

User access will be reviewed weekly to determine the appropriateness of access levels, and any changes needed to ensure access levels are appropriate will be made.

Accounts created for vendors or consultants to provide services must only be active during the service's execution and must be terminated immediately after the service period.

Temporary accounts for interns, temp employees, and consultants/contractors must have expiration dates.

12. INCIDENT RESPONSE

All security incidents involving Centenary IT systems, applications, and IT resources must reported to the IT Dept. for the proper handling and response to observed events.

All observed or suspected information security incidents or weaknesses must be reported to appropriate management and the CIO/designated security representative as quickly as possible.

The CIO must be notified of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.

The college will adhere to the state's SB205 Act 499 known as the "Database Security Breach Notification Law." The legislation requires notification to any Louisiana resident whose unencrypted "personal information" was or is reasonably believed to have been, acquired by an unauthorized person as a result of a "security breach."

13. THIRD-PARTY RISK MANAGEMENT

Centenary College will manage security risks that are introduced by third parties, including contracted vendor service providers and their members/participants. The intent is to ensure that the security of Centenary College's information and information assets are not reduced when sharing information with third parties or by the introduction of vendor products or services into the Centenary College environment.

Centenary College will take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the protection of customer information and Centenary College's sensitive data. Service providers will be required by contract to implement and maintain safeguards defined by Centenary College. Service providers will periodically be assessed based on the risk they present and the continued adequacy of their safeguards.

Third-party risk management must follow a risk management process which includes:

- Vendor selection
- Assess vendor risk
- Responding risk
- Monitor risk

14. VULNERABILITY MANAGEMENT

- All systems must be scanned for vulnerabilities before being installed in production and semi-annually thereafter.
- All production systems operating on the Centenary College network(s) will utilize the organization's designated endpoint detection and response (EDR) software.
- All EDR-equipped systems will forward alerts, logs, and events for centralized storage and monitoring.
- All systems are subject to annual penetration testing.
- Penetration tests are required annually for all critical environments/systems.
- Where the entity has outsourced a system to another entity or a third party, vulnerability scanning/penetration testing must be coordinated or evidence provided by the vendor tat they have completed testing.
- Scanning/testing and mitigation must be included in third party agreements.
- The output of the scans/penetration tests will be reviewed in a timely manner by the system owner. Copies of the scan report/penetration test must be shared with the ISO/designated security representative for evaluation of risk.
- Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created, and updated accordingly, to document the planned remedial actions to mitigate vulnerabilities.
- Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the CIO/designated security representative. The CIO must be notified in advance of any such tests. Any other attempts to perform such vulnerability scanning/penetration testing will be deemed an unauthorized access attempt.

- Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested and followed at all times to minimize the possibility of disruption.

15. AWARENESS AND TRAINING

Security awareness training and techniques are deployed across the organization to promote specific requirements to support adherence to this policy, the Acceptable Use Policy, and all other security policies and associated standards. Security awareness content must:

- Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.
- Address awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.
- Include security awareness training on recognizing and reporting potential indicators of insider threat.
- Provide role-based security training to personnel with assigned security roles and responsibilities:
- Designate personnel to receive initial and ongoing training in the employment and operation of environmental controls to include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.
- Provide training to its specified staff on how to recognize suspicious communications and anomalous behavior in organizational information systems.
- Designate personnel to document and monitor individual information system security training activities including basic security awareness training and specific information system security training.
- Security awareness training is required as part of initial training for new users, after information system changes, and then quarterly thereafter.
- Privacy awareness training must be delivered at a minimum to all parties interacting with non-public information.

16. COMPLIANCE

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

17. REVISION AND APPROVAL LOG

This standard shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
June 2024	PPAC approval	