cisecurity Information Technology Policy	**No:**
IT Policy: **Information Security**	**Updated:**
	Issued By: **Owner:**

1.0 Purpose and Benefits

This policy defines the mandatory minimum information security requirements for the entity as defined below in Section 3.0 Scope. Any entity may, based on its individual business needs and specific legal and federal requirements, exceed the security requirements put forth in this document, but must, at a minimum, achieve the security levels required by this policy.

This policy acts as an umbrella document to all other security policies and associated standards. This policy defines the responsibility to:

- protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets;
- manage the risk of security exposure or compromise;
- assure a secure and stable information technology (IT) environment;
- identify and respond to events involving information asset misuse, loss or unauthorized disclosure;
- monitor systems for anomalies that might indicate compromise; and
- promote and increase the awareness of information security.

Failure to secure and protect the confidentiality, integrity and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions and vital government functions; compromise data; and result in legal and regulatory non-compliance.

This policy benefits entities by defining a framework that will assure appropriate measures are in place to protect the confidentiality, integrity and availability of data; and assure staff and all other affiliates understand their role and responsibilities, have

adequate knowledge of security policy, procedures and practices and know how to protect information.

2.0 Authority

3.0 Scope

This policy encompasses all systems, automated and manual, for which the entity 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.

4.0 Information Statement

4.1 Organizational Security

a. Information security requires both an information risk management function and an information technology security function. Depending on the structure of the entity, an individual or group can serve in both roles or a separate individual or group can be designated for each role. It is recommended that these functions be performed by a high-level executive or a group that includes high level executives.

    1. Each entity must designate an individual or group to be responsible for the risk management function assuring that:

        i. 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

        ii. 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.

    2. Each entity must designate an individual or group to be responsible for the technical information security function. For purposes of clarity and readability, this policy will refer to the individual, or group, designated as the Information Security Officer (ISO)/designated security representative. This function will be responsible for evaluating and advising on information security risks.

b. Information security risk decisions must be made through consultation with both function areas described in **a.** above.

c. Although the technical information security function may be outsourced to third parties, each entity retains overall responsibility for the security of the information that it owns.

4.2 Functional Responsibilities

4.2.1 Executive management is responsible for:

1. evaluating and accepting risk on behalf of the entity;
2. identifying information security responsibilities and goals and integrating them into relevant processes;
3. supporting the consistent implementation of information security policies and standards;
4. supporting security through clear direction and demonstrated commitment of appropriate resources;
5. promoting awareness of information security best practices through the regular dissemination of materials provided by the ISO/designated security representative;
6. implementing 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;
7. implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization;
8. determining who will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data;
9. participating in the response to security incidents;
10. complying with notification requirements in the event of a breach of private information;
11. adhering to specific legal and regulatory requirements related to information security;
12. communicating legal and regulatory requirements to the ISO/designated security representative; and
13. 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.

4.2.2 The ISO/designated security representative is responsible for:

1. maintaining familiarity with business functions and requirements;

2. maintaining an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education (CPE) credits directly related to information security;

3. assessing compliance with information security policies and legal and regulatory information security requirements;

4. evaluating and understanding information security risks and how to appropriately manage those risks;

5. representing and assuring security architecture considerations are addressed;

6. advising on security issues related to procurement of products and services;

7. escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;

8. disseminating threat information to appropriate parties;

9. participating in the response to potential security incidents;

10. participating in the development of enterprise policies and standards that considers the entity's needs; and

11. promoting information security awareness.

4.2.3 IT management is responsible for:

1. 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;

2. providing resources needed to maintain a level of information security control consistent with this policy;

3. identifying and implementing all processes, policies and controls relative to security requirements defined by the business and this policy;

4. implementing the proper controls for information owned based on the classification designations;

5. providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);

6. 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

7. implementing business continuity and disaster recovery plans.

4.2.4 The workforce is responsible for:

1. understanding the baseline information security controls necessary to protect the confidentiality, integrity and availability of information entrusted;
2. protecting information and resources from unauthorized use or disclosure;
3. protecting personal, private, sensitive information from unauthorized use or disclosure;
4. abiding by *Acceptable Use of Information Technology Resources Policy*
5. reporting suspected information security incidents or weaknesses to the appropriate manager and ISO/designated security representative.

4.2.5 The CISO is responsible for:

1. providing in-house expertise as security consultants as needed;
2. developing the security program and strategy, including measures of effectiveness;
3. establishing and maintaining enterprise information security policy and standards;
4. assessing compliance with security policies and standards;
5. advising on secure system engineering;
6. providing incident response coordination and expertise;
7. monitoring networks for anomalies;
8. monitoring external sources for indications of data breaches, defacements, etc.
9. maintaining ongoing contact with security groups/associations and relevant authorities;
10. providing timely notification of current threats and vulnerabilities; and
11. providing awareness materials and training resources.

4.3 Separation of Duties

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

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

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

4.4 Information Risk Management

a. 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.

b. 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.

c. Entities are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.

d. Risk assessment results, and the decisions made based on these results, must be documented.

Associated Standard: Information Security Risk Management Standard;
Secure System Development Lifecycle (SSDLC) Standard

4.5 Information Classification and Handling

a. All information, which is created, acquired or used in support of business activities, must only be used for its intended business purpose.

b. All information assets must have an information owner established within the lines of business.

c. Information must be properly managed from its creation, through authorized use, to proper disposal.

d. All information must be classified on an ongoing basis based on its confidentiality, integrity and availability characteristics.

e. An information asset must be classified based on the highest level necessitated by its individual data elements.

f. 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.

g. 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.

h. 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.

i. Each classification has an approved set of baseline controls designed to protect these classifications and these controls must be followed.

j. The entity must communicate the requirements for secure handling of information to its workforce.

k. A written or electronic inventory of all information assets must be maintained.

l. Content made available to the general public must be reviewed according to a process that will be defined and approved by the entity. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.

m. PPI must not be made available without appropriate safeguards approved by the entity.

n. For non-public information to be released outside the entity or shared between other entities, a process must be established that, at a minimum:

    1. evaluates and documents the sensitivity of the information to be released or shared;

    2. identifies the responsibilities of each party for protecting the information;

    3. defines the minimum controls required to transmit and use the information;

    4. records the measures that each party has in place to protect the information;

    5. defines a method for compliance measurement;

    6. provides a signoff procedure for each party to accept responsibilities; and

    7. establishes a schedule and procedure for reviewing the controls.

Associated Standards: Information Classification Standard; Sanitization/Secure Disposal Standard

4.6 IT Asset Management

a. All IT hardware and software assets must be assigned to a designated business unit or individual.

b. 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.

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

Associated Standard: Secure Configuration Standard

4.7 Personnel Security

a. The workforce must receive general security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on specific security procedures, if required, must be completed before access is provided to specific entity sensitive information not covered in the general security training. All security training must be reinforced at least annually and must be tracked by the entity.

b. An entity must require its workforce to abide by the Acceptable Use of Information Technology Resources Policy, and an auditable process must be in place for users to acknowledge that they agree to abide by the policy's requirements.

c. All job positions must be evaluated by the to determine whether they require access to sensitive information and/or sensitive information technology assets.

d. For those job positions requiring access to sensitive information and sensitive information technology assets, entities must conduct workforce suitability determinations, unless prohibited from doing so by law, regulation or contract. Depending on the risk level, suitability determinations may include, as appropriate and permissible, evaluation of criminal history record information or other reports from federal, state and private sources that maintain public and non-public records. The suitability determination must provide reasonable grounds for the entity to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the entity.

e. A process must be established within the entity to repeat or review suitability determinations periodically and upon change of job duties or position.

f. Entities are responsible for ensuring all issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

Associated Standard: Account Management/Access Control Standard

4.8 Cyber Incident Management

a. Entities must have an incident response plan, consistent standards, to effectively respond to security incidents.

b. All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the ISO/designated security representative as quickly as possible. If a member of the workforce feels that cyber security concerns are not being appropriately addressed, they may confidentially contact the Security Operations Center directly.

c. The Security Operations Center 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.

Associated Standard: Cyber Incident Response Standard

4.9 Physical and Environmental Security

a. Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls.

b. A periodic risk assessment must be performed for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary. These measures must be implemented to mitigate the risks.

c. Information technology equipment must be physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities such as electrical supply and cabling infrastructure.

d. All information technology equipment and information media must be secured to prevent compromise of confidentiality, integrity, or availability in accordance with the classification of information contained therein.

e. Visitors to information processing and storage facilities, including maintenance personnel, must be escorted at all times.

Associated Standard: Information Security Risk Management Standard

4.10 Account Management and Access Control

a. All accounts must have an individual employee or group assigned to be responsible for account management. This may be a combination of the business unit and information technology (IT).

b. Except as described in the, Account Management/Access Control Standard, access to systems must be provided through the use of individually assigned unique identifiers, known as user-IDs.

c. Associated with each user-ID is an authentication token (e.g., password, key fob, biometric) which must be used to authenticate the identity of the person or system requesting access.

d. Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on the screen must be replaced with publicly viewable information (e.g., screen saver, blank screen, clock) during the session lock.

e. Automated techniques and controls must be implemented to terminate a session after specific conditions are met as defined in the Account Management/Access Control Standard.

f. Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.

g. Tokens must not be stored on paper, or in an electronic file, hand-held device or browser, unless they can be stored securely and the method of storing (e.g., password vault) has been approved by the ISO/designated security representative.

h. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.).

i. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with entity missions and business functions (i.e., least privilege).

j. Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail).

k. Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for business or other approved use consistent with policy, and that user activities may be monitored and the user should have no expectation of privacy.

l. Advance approval for any remote access connection must be provided by the entity. An assessment must be performed and documented to determine the scope and method of access, the technical and business risks involved and the contractual, process and technical controls required for such connection to take place.

m. All remote connections must be made through managed points-of-entry reviewed by the ISO/designated security representative.

n. Working from a remote location must be authorized by management and practices which assure the appropriate protection of data in remote environments must be shared with the individual prior to the individual being granted remote access.

Associated Standards: Account Management/Access Control Standard; Authentication Tokens Standard; Remote Access Standard; Security Logging Standard

4.11 Systems Security

a. Systems include but are not limited to servers, platforms, networks, communications, databases and software applications.

1. An individual or group must be assigned responsibility for maintenance and administration of any system deployed on behalf of the entity. A list of assigned individuals or groups must be centrally maintained.
2. Security must be considered at system inception and documented as part of the decision to create or modify a system.
3. All systems must be developed, maintained and decommissioned in accordance with a secure system development lifecycle (SSDLC).
4. Each system must have a set of controls commensurate with the classification of any data that is stored on or passes through the system.
5. All system clocks must synchronize to a centralized reference time source set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources.
6. Environments and test plans must be established to validate the system works as intended prior to deployment in production.
7. Separation of environments (e.g., development, test, quality assurance, production) is required, either logically or physically, including separate environmental identifications (e.g., desktop background, labels).
8. Formal change control procedures for all systems must be developed, implemented and enforced. At a minimum, any change that may affect the production environment and/or production data must be included.

    a. Databases and Software (including in-house or third party developed and commercial off the shelf (COTS):
        1. All software written for or deployed on systems must incorporate secure coding practices, to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.
        2. Once test data is developed, it must be protected and controlled for the life of the testing in accordance with the classification of the data.
        3. Production data may be used for testing only if a business case is documented and approved in writing by the information owner and the following controls are applied:
            i. All security measures, including but not limited to access controls, system configurations and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed; or
            ii. sensitive data is masked or overwritten with fictional information.
        4. Where technically feasible, development software and tools must not be maintained on production systems.

5. Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software.
6. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
7. Privileged access to production systems by development staff must be restricted.
8. Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.

b. Network Systems:

1. Connections between systems must be authorized by the executive management of all relevant entities and protected by the implementation of appropriate controls.
2. All connections and their configurations must be documented and the documentation must be reviewed by the information owner and the ISO/designated security representative annually, at a minimum, to assure:
    i. the business case for the connection is still valid and the connection is still required; and
    ii. the security controls in place (filters, rules, access control lists, etc.) are appropriate and functioning correctly.
3. A network architecture must be maintained that includes, at a minimum, tiered network segmentation between:
    i. Internet accessible systems and internal systems;
    ii. systems with high security categorizations (e.g., mission critical, systems containing PII) and other systems; and
    iii. user and server segments.
4. Network management must be performed from a secure, dedicated network.
5. Authentication is required for all users connecting to internal systems.
6. Network authentication is required for all devices connecting to internal networks.
7. Only authorized individuals or business units may capture or monitor network traffic.
8. A risk assessment must be performed in consultation with the ISO/designated security representative before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.

Associated Standards: Secure System Development Lifecycle Standard; Secure Coding Standard; Security Logging Standard; Secure Configuration Management Standard

4.12 Collaborative Computing Devices

a. Collaborative computing devices must:

    1. prohibit remote activation; and

    2. provide users physically present at the devices with an explicit indication of use.

b. Must provide simple methods to physically disconnect collaborative computing devices.

4.13 Vulnerability Management

a. All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter.

b. All systems are subject to periodic penetration testing.

c. Penetration tests are required periodically for all critical environments/systems.

d. Where the entity has outsourced a system to another entity or a third party, vulnerability scanning/penetration testing must be coordinated.

e. Scanning/testing and mitigation must be included in third party agreements.

f. 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.

g. 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.

h. Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the ISO/designated security representative. The CISO 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.

i. 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.

Associated Standards: Patch Management Standard; Vulnerability Scanning Standard

4.14 Operations Security

a. All systems and the physical facilities in which they are stored must have documented operating instructions, management processes and formal incident management procedures related to information security matters which define roles and responsibilities of affected individuals who operate or use them.

b. System configurations must follow approved configuration standards.

c. Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.

d. Where the entity provides a server, application or network service to another entity, operational and management responsibilities must be coordinated by all impacted entities.

e. Host based firewalls must be installed and enabled on all workstations to protect from threats and to restrict access to only that which is needed

f. Controls must be implemented (e.g., anti-virus, software integrity checkers, web filtering) across systems where technically feasible to prevent and detect the introduction of malicious code or other threats.

g. Controls must be implemented to disable automatic execution of content from removable media.

h. Controls must be implemented to limit storage of information to authorized locations.

i. Controls must be in place to allow only approved software to run on a system and prevent execution of all other software.

j. All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.

k. All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically possible.

l. Systems which can no longer be supported or patched to current versions must be removed.

m. Systems and applications must be monitored and analyzed to detect deviation from the access control requirements outlined in this policy and the Security Logging Standard, and record events to provide evidence and to reconstruct lost or damaged data.

n. Audit logs recording exceptions and other security-relevant events must be produced, protected and kept consistent with record retention schedules and requirements.

o. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound and internal network traffic.

p. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.

q. Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly. At a se

    1. An evaluation of the criticality of systems used in information processing (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).

    2. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.

r. Backup copies of entity information, software, and system images must be taken regularly in accordance with the entity's defined requirements.

s. Backups and restoration must be tested regularly. Separation of duties must be applied to these functions.

t. Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.

Associated Standards: Secure Configuration Management Standard; Security Logging Standard; Cyber Incident Response Standard; Account Management/Access Control Standard

5.0 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.

6.0 Definitions of Key Terms

Term	Definition

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:
cisecurity@ cisecurity.com

8.0 Revision History

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

Date	Description of Change	Reviewer

9.0 Related Documents

National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

Internal Revenue Service Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies