**Enterprise Information Security Policy(ISMS)**

|  |
| --- |
| **Enterprise Information Security Policy**  |
| **Compliance** | **NIST:** ID.GV-1, ID.GV-2, ID.GV-3, ID.BE-1, ID.BE-2, ID.BE-3, RS.CO- |
| **Mandates:** | 1, PR.IP-5 |
|  | **NYDFS:** 500.03(a) |
|  | **ISO 27001:** 5.1.1, 5.1.2, 6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5, 7.2.1, 7.2.3, |
|  | 18.1.1, 18.1.2, 18.1.3, 18.1.4, 18.1.5, 18.2.1, 18.2.2, 18.2.3 |

|  |  |
| --- | --- |
|  | **NAIC:** 4(a), 4(b)(1), 4(b)(2), 4(b)(3), 4(b)(4), 4(e)1, 4(e)2, 4(e)3, 4(g), 4(i)**HIPAA:** 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(C)**PCI-DSS 3.2:** 12.1, 12.1.1,12.5.1 |
| **Department Owner:** | Enterprise Information Security Office (EISO) | **Last Revised:** | Date  |

# **Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Approver(s)** | **Effective Date** | **Change Description** |
| 1.0 | E-ISO | Date | Document Creation |

**Introduction:**

This Enterprise Information Security Policy defines enterprise-wide minimum information security requirements for an effective security program. All employees and contractors shall apply information security in accordance with the established Policies, Standards, and Procedures of the organization. The minimum requirements defined in this policy may be exceeded as required. Any non-compliance with EISO Policy and Standards shall be enforced through the Corrective Notification Process as outlined within the Employee Handbook.

## **Scope**

This policy applies to all IT Asset Owners, Control Owners, Data Owners, Authorized Users within Enterprise, and Contractors. This policy governs controls around restriction of access to Enterprise IT Assets and information, and functionality on a need to know basis to assist in protecting information.

## **Responsible Parties**

The relevant roles and responsibilities are defined as follows:

* + 1. Enterprise Information Security Office (E-ISO): is responsible for setting an enterprise strategic vision and direction for Enterprise’s information security program. The **Information Security Management System (ISMS)** will document the mandate and scope of the respective programs.
		2. Chief Information Security Officer (CISO): is responsible for overall enterprise- level, including all divisions, accountability and responsibility for the program and drives the strategy, direction, and framework using a risk-based approach, and operational management of selected security controls within the organization.
		3. Business Information Security Officer (BISO): is responsible for providing independent and objective oversight and monitoring within the Business

area, driving achievement and strategic alignment of business and security objectives, and escalating exceptions and incidents to the CISO.

* + 1. Asset Owner: is responsible for the management and configuration of IT Assets to ensure compliance with this policy.
		2. Control Owner: is responsible for coordinating with the IT Asset Owner and

the Data Owner to ensure controls associated with this policy are implemented and maintained. The Control Owner will provide feedback and input to the IT Asset Owner and Data Owner as needed.

* + 1. Data Owner: is responsible for coordinating with the IT Asset Owner and Control Owner to ensure applicable controls are implemented commensurate to the risk of the data being processed.
		2. Authorized User: is responsible for acting in compliance with this policy and ensuring the security of their IT Assets. Authorized Users are also responsible for reporting any potential or real risks they are aware of through the prescribed channels.
		3. Privileged User is defined as an employee, consultant, contractor, business partner or other individual who has been authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
		4. Data Custodian is responsible for the storage and safeguarding of computerized data.
		5. Asset Custodian is responsible for the management and protection of organizational assets.
		6. Data Process Owner is responsible for the integrity, accurate reporting, and use of computerized data processes.

## **Reviews and Changes to the Standard**

Enterprise shall review and improve all standards annually, or when there are significant changes to the environment. This policy shall be evaluated and adjusted at least annually due to testing, monitoring, changes in applicable laws and regulation, and adoption of best practices. The Enterprise Information Security Office is responsible for approving all changes.

## **Standard Compliance and Security Exceptions**

Compliance to this policy is mandatory for all responsible parties. Enterprise may conduct periodic assessments and audits at its discretion or when significant organizational or regulatory changes occur to assess compliance with this policy.

# **Security Program**

The objective of this policy is to provide management direction and support for cybersecurity in accordance with business requirements and relevant laws and regulations. An Information Security Management System (ISMS) focuses on cybersecurity management and technology-related risks. The governing principle behind Enterprise’s ISMS is that the ISMS shall remain current to be effective and efficient in the long-term, adapting to changes in the internal organization, external environment, and applicable legal and regulatory requirements.

In accordance with leading practices, Enterprise’s ISMS incorporates the following approach:

1. **Plan:** This phase involves designing the ISMS, assessing IT-related risks, and selecting appropriate controls.
2. **Do:** This phase involves implementing and operating the appropriate security controls.
3. **Check:** This phase involves reviewing and evaluating the performance

(efficiency and effectiveness) of the ISMS.

1. **Act:** This involves making changes when necessary to bring the ISMS back to optimal performance.

Information security documentation is comprised of four main parts:

1. Core policy that establishes management’s intent
2. Standards that provides quantifiable requirements to be met
3. Procedures that establish how tasks shall be performed to meet the requirements established in standards
4. Guidelines provide recommended guidance to meet all quantifiable requirements as outlined in the standards

# **Policy Statements**

## **IT Asset Management**

**Management Intent:** Asset and Inventory management is key to mature security and management practices, providing context for all IT Security Policy statements and Standard requirements. Without an accurate inventory, processes such as vulnerability management are difficult to implement. Based on Data Classification, IT Asset Owners shall implement appropriate ISMS and Data Handling controls to maintain Confidentiality, Integrity and Availability of Enterprise Data.

* + 1. **Statement:** In the context of this policy, an IT asset is any Enterprise owned or managed device or service that connects to or is used by Enterprise in its business. Enterprise shall protect its assets and data by implementing and maintaining appropriate IT Asset Management (ITAM) business practices across the enterprise.

## **Business Continuity & Disaster Recovery**

**Management Intent:** Service availability is critical for Enterprise’s Information Technology communications, infrastructure, systems, and applications. This Policy ensures that processes are in place to recover from system and environmental failures, and that regular testing of these processes is established.

Backups are an integral piece to an effective continuity and recovery program, and an essential safeguard to ensure availability of Enterprise’s information. Data Backups are considered a preventative measure to protect against loss of data resulting from system failure, malicious attacks, and system or human error.

* + 1. **Statement:** Enterprise shall establish and manage resilience capabilities for maintaining the continuity of critical operations and to ensure the availability of critical technology resources during adverse conditions. Processes shall be in place to enable the recovery of business-critical services in a timely manner to minimize the effect of disruptions, and to maintain resilience before, during, and after the incident.

## **Change Management**

**Management Intent:** The Enterprise change management process ensures stability and availability of related information technology communication systems. Secure practices including reviews during changes are necessary to ensure service availability. Integrating risk management practices into the change management process is key to an effective and successful program.

* + 1. **Statement:** All technology changes to production environments shall follow a standard process to reduce the risk associated with change. Enterprise requires active stakeholder involvement to ensure changes are appropriately tested, validated and documented before implementing any change on a production network. Risk and impact of each request shall be evaluated, and the proposed risk mitigation solution shall be documented and approved.

## **Risk Management**

**Management Intent:** Risk Management is at the core of the Information Security Management System (ISMS). Enabling Enterprise to identify, assess, and evaluate risk enabling effective management of information security vulnerabilities and threats to information assets that could adversely affect business operations.

An effective risk management program ensures that cybersecurity-related risk is visible to and understood by the business units that own the assets and/or processes involved. Since the E-ISO team facilitates and educates the management of risk, business units and other key stakeholders are expected to be active participants in Enterprise’s risk management.

* + 1. **Statement:** Information security risk shall be identified, mitigated and monitored through a formalized risk management process. The management of risk at the appropriate level of corporate management is of critical importance to Enterprise’s long-term success. Therefore, Enterprise shall periodically assess the risk to operations, assets, and data that is associated with the processing, storage, or transmission of information to support Enterprise’s business processes and take appropriate action to remediate unacceptable risks.

## **Compliance Management**

**Management Intent:** Compliance with Enterprise’s ISMS shall be measured and monitored to ensure all Divisions within Enterprise abide by the security controls outlined in the ISMS. Compliance with applicable statutory, regulatory and contractual compliance obligations will also be measured to ensure Enterprise is aligned with all applicable legal requirements. The CISO shall also report, at least annually, the current state of the organizational security posture, and includes future state initiatives.

* + 1. **Statement:** Enterprise shall protect the confidentiality, integrity, and availability of its data and systems, regardless of how its data is created, distributed, or stored. Security controls shall ensure appropriate safeguards are in place to protect sensitive business data against loss, unauthorized access or disclosure in accordance with all statutory, regulatory and contractual obligations.

## **Data Protection & Classification**

**Management Intent:** The purpose of a mature data classification and handling scheme is to ensure that technology assets and data is properly classified and measures are implemented to protect Enterprise’s data from unauthorized disclosure, regardless if it is being transmitted or stored. Applicable statutory, regulatory and contractual compliance obligations dictate the safeguards that shall be in place to protect the confidentiality, integrity and availability of data.

* + 1. **Statement:** In accordance with all applicable legal requirements, Enterprise shall protect data in both hardcopy and digital form by limiting access to authorized users and utilize methods of sanitizing or destroying media so that data recovery is technically infeasible.

## **Configuration Management**

**Management Intent:** The purpose of a configuration management policy is to establish and maintain the integrity of systems. Without properly documented and implemented configuration management controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur or malicious code could be introduced.

* + 1. **Statement:** All technology platforms shall adhere to configuration management requirements. Enterprise shall maintain accurate inventories of

its technology platforms and enforce security configuration settings for those technology platforms used in support of Enterprise’s business operations.

## **Logging and Monitoring**

**Management Intent:** The purpose of logging and monitoring is to establish and maintain situational awareness across the enterprise through the centralized collection and review of all security-related event logs. Without comprehensive visibility into the infrastructure, operating system, databases, applications, and other logs, Enterprise will endeavor to identify gaps within its situational awareness that could lead to system compromise and/or data exfiltration.

* + 1. **Statement:** Through ongoing and continuous logging and monitoring of Enterprise’s technology assets can situation awareness of cybersecurity events be maintained. Therefore, technology assets shall adhere to configuration management requirements to log security events and forward those events to allow for the centralized monitoring and review of logs to identify anomalous behavior so that appropriate steps can be taken to remediate potential cybersecurity incidents.

## **Cryptographic Protections**

**Management Intent:** Cryptographic protections and practices will be designed to deliver the confidentiality of Enterprise’s data through implementing appropriate cryptographic technologies to protect systems and data.

* + 1. **Statement:** Appropriate cryptographic safeguards shall be used to protect sensitive business data as defined in the data classification policy and standard against loss, unauthorized access, and/or disclosure. This applies to all data, regardless if it is at rest or in transit.

## **Endpoint Security**

**Management Intent:** Endpoints are the primary gateway to Enterprise’s data and business applications. Implementation of endpoint security controls helps ensure that endpoint devices are appropriately protected from reasonable threats to the confidentiality, integrity, availability, privacy, safety, and resilience of the device and its data. Applicable statutory, regulatory and contractual compliance obligations dictate the safeguards that shall be in place to protect Enterprise’s endpoints.

* + 1. **Statement:** Enterprise shall implement the concept of least functionality for its technology endpoints and proactively govern security mechanisms to keep its technology assets secure from evolving threats, and unauthorized disclosure and/or modification of Enterprise’s data.

## **Human Resources Security**

**Management Intent:** In support of the Human Resources Policies, the purpose of the Human Resources Security policy is to create a security-minded workforce and an environment that is conducive to innovation, considering issues such as culture, reward, and collaboration.

* + 1. **Statement:** Enterprise shall ensure industry-recognized leading practices for cybersecurity are incorporated into Human Resources personnel management practices and followed before, during, and after the termination of employment of all Enterprise employees. Disciplinary action for workforce members who have access to confidential and/or restricted information shall come from Human Resources in accordance with the Employee Handbook

## **Identification and Authentication Management**

**Management Intent:** The Identification & Authentication practice is a preventive measure designed so that only authorized users are granted access to Enterprise’s

systems. Unauthorized access enables a malicious or accidental security breach. Breach of access could impact the confidentiality, availability, and/or integrity of sensitive information potentially resulting in productivity, reputational or financial loss. Implementing the concept of “least privilege” through limiting access to Enterprise’s systems and data to only authorized users is key to a successful program.

* + 1. **Statement:** Enterprise shall implement the principle of “least privilege” within logical access control mechanisms so that only authorized users can gain access to Enterprise’s systems and data. All user access related requests shall be logged, assessed, and approved in accordance with defined **Access Management and Controls Standard**.

## **Incident Management & Response**

**Management Intent:** The purpose of the Incident Response policy is to establish and maintain a capability to guide Enterprise’s response when security-related incidents occur. Providing preventive, corrective, and detective measures ensures a consistent and effective approach to the management of information security incidents. This includes communication of events and weaknesses, such as breach of access. A mature program and toolset with established processes will help contain, preserve and limit any damage resulting from a security incident.

* + 1. **Statement:** Enterprise shall maintain a cybersecurity incident handling capability that includes adequate preparation, detection, analysis, containment, recovery and reporting activities. Incident detection mechanisms such as security event logging and antivirus shall be implemented for all IT systems to support this policy. All potential security incidents shall be handled according to a formalized process

## **Network Security**

**Management Intent:** The purpose of the Network Security policy is to ensure sufficient security controls are in place to protect the confidentiality, integrity, and

availability of Enterprise’s communications and systems, as well as to provide situational awareness of activity on Enterprise’s networks. Network infrastructure components provide essential connectivity between internal and external systems. To provide mitigation against malicious activity, secure boundaries and connections need to be defined and managed.

* + 1. **Statement:** Enterprise shall implement the concept of “least functionality” for its network infrastructure and proactively govern security mechanisms to keep its networks secure from evolving threats, while providing situational awareness of network activities so that proactive measures can be implemented to address evolving threats.

## **Physical Security**

**Management Intent:** Physical security is important for critical infrastructure that shall be protected from physical or environmental damage. Physical security is a preventive control intended to minimize risk to Enterprise systems and data by addressing applicable physical security and environmental concerns.

* + 1. **Statement:** Enterprise shall implement appropriate physical controls to limit access to systems, equipment, and the operating environments to authorized individuals. Enterprise shall also provide appropriate environmental controls in facilities containing systems to ensure sufficient environmental conditions exist to avoid preventable hardware failures and service interruptions.

## **Training and Awareness**

**Management Intent:** The purpose of the security awareness & training policy is to develop a security and privacy-minded workforce.

* + 1. **Statement:** Enterprise shall ensure that users are made aware of the security and privacy risks associated with their roles and that users understand the

applicable statutory, regulatory and contractual compliance requirements related to the security and privacy of systems and data within their sphere of influence.

## **IT System Acquisition & Development**

**Management Intent:** The purpose of the Technology Development & Acquisition policy is to ensure secure technologies are developed and/or acquired in accordance with applicable statutory, regulatory and contractual compliance requirements. IT systems are susceptible to attack and therefore security controls shall be embedded throughout the whole system acquisition and development lifecycle.

* + 1. **Statement:** Enterprise shall implement the principles of “least privilege” and “least functionality” in the development and implementation of technology, regardless if it is internally-developed or acquired from a third-party. Technology development and acquisition shall employ adequate security measures during all phases of the System Development Life Cycle (SDLC) to ensure security and privacy-related risks are identified and appropriately remediated.

## **Third Party Risk Management**

**Management Intent:** The purpose of the Third-Party Risk Management policy is to ensure that security and privacy risks are considered, minimized, and/or avoided whenever possible. Agreements should enforce appropriate information security controls in accordance with applicable statutory, regulatory and contractual compliance requirements. applicable statutory, regulatory and contractual compliance requirements.

* + 1. **Statement:** Enterprise shall assess the cybersecurity and privacy risks posed by both its current and potential third-party providers. It is imperative that Enterprise’s third-parties implement mechanisms to identify and remediate deficiencies and/or vulnerabilities on an ongoing basis, to ensure the

continued effectiveness of security and privacy controls. As third-party providers’ technology and processes evolve over time, Enterprise shall ensure the appropriate levels of due diligence is applied to validate that appropriate security controls are effective.

## **Vulnerability Management**

**Management Intent:** The purpose of the Vulnerability & Patch Management policy is to proactively manage the risks associated with technical vulnerability management. All systems are susceptible to vulnerability and under constant threat from malicious exploitation that may result in the compromise of confidentiality, integrity or availability of Enterprise’s information or systems. Successful exploitation can potentially result in productivity, reputational, and/or financial loss.

Proper vulnerability management involves alerting and responding to identified and potential violations or security threats in a timely, measured, and prioritized manner. To prevent or limit the damage. Vulnerability management is considered a preventive and corrective measure.

* + 1. **Statement:** Vulnerability management is a continuous process that requires Enterprise to proactively manage vulnerabilities both in how its assets are configured and the level of currency in software patching. Therefore, Enterprise shall apply a risk-based approach to minimize its attack surface area through aggressive vulnerability management and patching operations.

## **Cloud Security**

**Management Intent:** Enterprise utilizes cloud solutions to deliver business solutions and functionality. Expectations of cloud service providers are to meet best practice security controls and access requirements ensuring all Enterprise information and system controls are met.

* + 1. **Statement:** Enterprise cloud-based services shall be consumed following a formalized risk assessment to identify the necessary security controls that shall be established by the Cloud Service Provider and Enterprise to manage security risks to an acceptable level.

## **Application Security**

**Management Intent:** Applications are used extensively across Enterprise for the delivery of business services and information. They also represent one of the highest exposures to security attacks. Given the number of security exploits that exist for web interfaces, secure design, implementation and monitoring are essential.

* + 1. **Statement:** Applications need to be designed, built, and tested (verified) to ensure security is applied at all layers of the application and technology. Assessment and design guidelines provide controls to be followed when developing Enterprise applications, especially those that are internet-facing (Web).

# **Appendix**

## **A - Referenced Documentation**

|  |  |
| --- | --- |
| **Section** | **Documentation** |
| 4.1 | S16\_Asset Management Standard |
| 4.2 | S11\_BC/DR Management Standard |
| 4.3 | S10\_System Configuration and Hardening Standard |
| 4.4 | S13\_Information Risk Management Standard |
| 4.5 | S13\_Information Risk Management Standard |
| 4.6 | S03\_Data Protection Standard |

|  |  |
| --- | --- |
| 4.7 | S10\_System Configuration and Hardening Standard |
| 4.8 | S07\_Security Logging and Monitoring Standard |
| 4.9 | S05\_Encryption and De-Identification Standard |
| 4.10 | S10\_System Configuration and Hardening Standard |
| 4.12 | S02\_Access Management and Controls Standard |
| 4.13 | S08\_Incident Response Standard |
| 4.14 | S12\_Communications Security Standard |
| 4.15 | S15\_Physical and Environmental Security Standard |
| 4.16 | S01\_Security Awareness and Training Standard |
| 4.17 | S14\_Secure Coding and SDLC Standard |
| 4.18 | S13\_Information Risk Management Standard |
| 4.19 | S06\_Vulnerability and Patch Management standard |
| 4.20 | S09\_Cloud Security Standard |
| 4.21 | S14\_Secure Coding and SDLC Standard |

* 1. **Terms and Definitions**

A full set of terms and definitions are provided in the **Enterprise Information Security Policy** document.

Below are some useful terms and definitions utilized in this document:

* + 1. “Information Technology Asset (IT Asset)” is defined as hardware, software, or Information Technology Asset in any form to support Enterprise’s business operations, whether belonging or entrusted to Enterprise, including information about employees, business operations and plans, customers, and business partners.
		2. “Security Exception” is defined as any non-compliance to this policy that has been approved in accordance with the **Information Security Exception Standard**.
		3. “Remote Access” is defined as Authorized User access to Enterprise IT Assets from any point outside of the Enterprise network. Remote Access devices include but are not limited to; Citrix, client based VPN, Outlook Web Access, mobile devices, and cloud-based applications.
		4. “Protected Information System” is defined as an information system that processes, stores, or transmits Confidential information. Additionally, any system that is internet-facing will be classified within this category.
		5. “Restricted Information System” is defined as an information system that processes, stores, or transmits Restricted Use information.
		6. “Unrestricted Information System” is defined as an information system that

processes, stores, or transmits Public information.

* + 1. “Public” is defined as information that is publicly available, routine, short- term, and day-to-day and is freely discussed. Disclosure of public domain information outside the company has no adverse impact on the Enterprise organization, its employees, clients, or business partners.
		2. “Restricted Use” is defined as information to be used by Enterprise and those with whom Enterprise is, or will, conducting business. It is restricted to use on a need-to-know basis. Public access to this information is to be restricted, but if this information became public, the consequences are not critical.
		3. “Confidential” is defined as information that is not publicly available where the tampering with, unauthorized disclosure, access, or use of which, would cause a material adverse impact to the business, operations, or security of Enterprise.