Author/Date	
Systems Owner Approval / Date	
Quality Approval / Date	

1. **Purpose:**
   1.1. The purpose of this policy is to define the cybersecurity requirements designed to protect the information assets of <COMPANY NAME>. Any business unit/department may exceed the security requirements defined within this procedure to meet its individual business needs or to satisfy specific legal requirements. However, all business units/departments must, at a minimum, achieve the security levels defined herein.
2. **Scope:**
   2.1. This policy is applicable to entities, staff and external consultants who have access to or manage <COMPANY NAME> Information. This policy encompasses all information systems both hosted or on premise for which <COMPANY NAME> has administrative responsibility. Where conflict exists between this policy and departmental policies, the more restrictive policy will take precedence.
   2.2. This policy must be communicated by supervisors to all employees and all external consultants and/or contractors who have access to or manage digital information assets on behalf of the company. This policy is technology independent and does not include implementation standards, processes or procedures
3. **Definitions**

Term	Definition
Authorized User	Refers to any individual granted access to corporate information systems
Credentials	Refers to the unique username and password provided to each authorize users to access corporate systems
Cyber Defense	Means acting in anticipation to oppose an attack against computers and networks.
Cybersecurity	The protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide
Data Integration Model	A logical construct that describes the data entities of a database and the relationship among those entities.

Term	Definition
Data Ownership	The individual(s) with stewardship responsibilities for portions of enterprise data.
Data Warehouse	A system used for reporting data analysis and is considered a core component of business intelligence environment. Data warehouses are central repositories of integrated data from one or more disparate data sources.
Database Administration	The function of managing and maintaining database management systems (DBMS) software.
Digital Information	Is defined as the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by computer automated means.
Digital Systems	Refers to the computer platform on which digital information is stored and used.
Highly Sensitive Information	Refers to information that is considered proprietary or confidential.
Information Assets	Refers to the data and resources owned and protected by the company
Metadata Repository	Refers to a database system that contains descriptive information about enterprise data and administrative systems. The repository is a complementary facet of a data warehouse.
System Administration	The function of maintaining and operating hardware and software platforms.

4. Responsibility:

Role	Responsibilities
Chief Information Officer (CIO) Or Designate	• Responsible for oversight and management of corporate data systems • Responsible for the procurement and service level agreements for all corporate business systems • Responsible for the information system strategy corporate wide

Role	Responsibilities
	• Responsible for establishing cybersecurity policy across the Corporation
Database Administrator	• Establish formal guidelines for database management systems • Management of all cybersecurity related to database administration including physical security, backup and recovery, granting and terminating access privileges and administration of general controls over all database information
Authorized User	• Day-to-day use of the system • Protection of login credentials
Data Experts/Managers	• Day-to-day responsibility for managing business processes • Establish business rules for data capture, maintenance, and dissemination
Steering Committee	• Make recommendations for cybersecurity management • Establish and document data management standards and procedures including integration standards • Ensure that individual responsibilities and procedures are clearly outlined and appropriately communicated
Information Technology Manager	• Management of computer systems infrastructure and network • Conduct cybersecurity assessment • Continuous monitoring for cybersecurity threats • Management oversight and remediation of cybersecurity breaches • Allocation of personnel to manage cybersecurity events
Validation Project Manager	• Allocation of validation resources to conduct computer system validation • Development of validation test plan that includes cybersecurity testing • Maintain the validated state through periodic regression testing and cybersecurity compliance monitoring
Validation Engineer	• Validation testing of all cybersecurity controls • Maintaining the validated state of all secure corporate systems

Role	Responsibilities
Employees	• Responsible for reading and understanding this policy • Protection of corporate information and resources • Protection of all password and user credentials issued for corporate business systems • Reporting of any variances from this procedure to supervisors and/ or executive management
Supervisors/Managers	• Responsible for the dissemination, communication of and compliance with this procedure • Education of employees with respect to information security issues and retention policies • Notify system administrators when staff members terminate employment
System Administrators	• Responsible for: • Administering security tools • Auditing security practices • Identifying and analyzing security threats and solutions • Implementing specific security controls • Responding to security violations • Administration over user ids and passwords • Management of processes for reviewing, logging, implementing access rights, emergency privileges, exception handling, and reporting requirements

5. Policy and Procedure

5.1. POLICY

5.1.1. It is our corporate policy to establish a multi-tiered cybersecurity risk management process to protect enterprise information assets. Risk associated with vulnerabilities inherent in advanced computer business systems must be considered in the implementation of capabilities to achieve business objectives.

5.1.2. It is our policy to address risk management as early as possible in the acquisition and deployment of business information systems. Cybersecurity features must be fully integrated into the system lifecycles and will be a visible element of organizational IT portfolios.

5.1.3. Cyberspace defense will be employed to protect, detect, characterize, counter, and mitigate unauthorized activity and vulnerabilities on corporate information networks. Cyberspace defense information will be shared with all appropriate personnel in support of enterprise-wide situational awareness.

5.1.4. The primary objectives of this policy are as follows:

5.1.4.1. Manage the risk of security exposure or compromise of <COMPANY NAME> Information assets;

5.1.4.2. Designate responsibilities for the protection of <COMPANY NAME> information;

5.1.4.3. Optimize the integrity and reliability of <COMPANY NAME>. information assets

5.1.4.4. Reduce opportunities for the introduction of errors in information assets supporting <COMPANY NAME> business processes;

5.1.4.5. Protect <COMPANY NAME> senior management and staff and preserve senior management options in the event of information asset misuse, loss or unauthorized disclosure;

5.1.4.6. Promote and increase the awareness of information security at <COMPANY NAME>.

5.2. PROCEDURE

5.2.1. General

5.2.1.1. Cybersecurity procedures shall apply to all IT business systems that receive, process, store, display, or transmits any corporate information.

5.2.1.2. Cybersecurity requirements must be identified and included in the design, development, acquisition, installation, operation, upgrade, validation, or replacement of all business systems either purchased or developed for <COMPANY NAME>.

5.2.1.3. Enterprise applications, due to the regulatory or cGMP information in them, may require special management oversight due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information within the application and should be treated as mission-critical. Mission-critical software applications may be a single software application or multiple software applications that are related to a single business function i.e. supply chain management.

5.2.1.4. All business applications, regardless of whether they are enterprise applications or not, require an appropriate level of protection. Adequate security for non-enterprise applications may be provided by security of the environment in which they operate.

5.2.1.5. When possible, capabilities should be developed as applications hosted in existing authorize computing environments rather than designated as enterprise applications requiring new/separate authorizations.

5.2.1.6. The corporate IT department will resolve any disputes regarding whether an application is an enterprise application.

5.2.2. Personnel Security Policy

5.2.2.1. A Human Resources Information Security program is designed and established to reduce the risks of human error, theft or misuse of corporate information assets.

5.2.2.2. Security responsibilities shall be defined and addressed at the employee hiring stage, included in contracts with third parties, and monitored by throughout the course of employment.

5.2.2.3. The company follows State guidelines with respect to pre-employment screening. Additional pre-screening check shall include, but are not limited to the following:

- Previous employment;
- criminal records as authorized by federal and state laws;
- A check (for completeness and accuracy) of the applicants' curriculum vitae (CV);
- confirmation of claimed academic and professional qualifications;
- Independent identity checks (passport, visa or similar documents) consistent with federal state laws.

5.2.3. Cybersecurity Risk Management

5.2.3.1. Managing cybersecurity risk is a complex, multi-faceted undertaking that requires the involvement of the entire organization, from senior management to individuals developing, implementing, and operating corporate business systems.

5.2.3.2. Cybersecurity risk management is a subset of the overall risk management process for corporate business systems.

5.2.3.3. The risk assessment process extends to the logistics support of fielded equipment and the need to maintain the integrity of supply sources.

5.2.3.4. This policy assumes the adoption of the NIST SP 800 – 37 publication to address risk management as defined herein.

5.2.3.5. Integrated organization-wide risk management. Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization. The figure 1 below illustrates a three-tiered approach to risk management that addresses risk related concerns at the organizational level, business process level and the IT level.

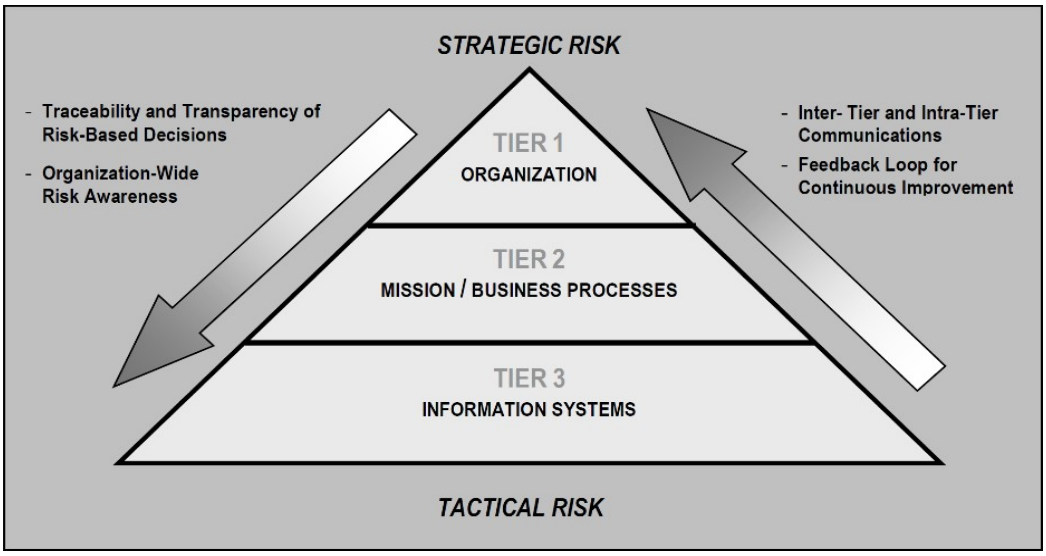

Figure 1 - Enterprise Risk Management

5.2.3.6. Risk management at tier 1 addresses risk from an organizational perspective. As part of the feedback loop tier 1 risk management is informed and influenced by risk decisions made in tiers two and three.

5.2.3.7. A comprehensive IT security governance structure shall be established that provides assurance that IT strategies are aligned and support business objectives and are consistent with applicable laws and regulations through adherence to policies and internal controls.

5.2.3.8. Risk management task shall begin early in the system development lifecycle process and are important in shaping the security capabilities of the business system. It should be noted that if these tasks are not adequately performed during the initiation, development, and acquisition phases of the system development lifecycle the task will, by necessity, be undertaken later in the life cycle which may prove to be costlier and time-consuming to implement and could negatively impact the performance of the system.

5.2.3.9. Cybersecurity risk management shall be planned for and documented in a cybersecurity strategy. Periodic reviews of the strategy and associated system engineering documentation shall evaluate the status of cybersecurity solutions as part of the overall systems development process.

5.2.3.10. Risk management shall continue during sustained operations. This may include the application of new or revised security controls prior to the integration of new IT services or products into an existing operational business system to maintain the security of the operational environment.

5.2.3.11. Risk assessment. Conducting a formal risk assessment is a key step in in the organizational risk management process. Risk assessments shall be performed in accordance with processes described in the risk management SOP FE-054. All risk

factors assessed must ensure reciprocity and ease of sharing risk information. The robustness of the risk assessments may be tailored to accommodate resource constraints and the availability of detailed risk factor information (e.g., threat data). However, any tailoring must be clearly explained in the risk assessment reports to ensure that reviewers understand to what degree they can rely on the results of the risk assessments.

5.2.4. Security controls. Security controls shall be expressed in a specified format (e.g., a control number, a control name, control text, and enhancement text).

5.2.4.1. All security controls shall be published in the security plan for the validated system with supporting validation procedures.

5.2.4.2. Implementation guidance and validation procedures shall be developed by the CIO with direct support from the validation team

5.2.5. Integration and Interoperability

5.2.5.1. Net-Centric Operations. A net-centric model provides people, services, and platforms the ability to discover one another and connect to form new capabilities or teams without being constrained by a geographic, organizational, or technical barriers. The net-centric model allows people, services, and platforms to work together to achieve shared ends. To be net-centric, cybersecurity will be designed, organized, and managed to enable them to work together in any combination that events demand and maintain an expected level of readiness so that all required cybersecurity assets can be brought to bear in a rapid and flexible manner to meet new or changing needs.

5.2.5.2. Integration. Cybersecurity must be fully integrated into system lifecycle, so it would be a visible element of organizational, joint, and component architectures, capability identification and development processes, integrated testing, information technology portfolios, acquisition, operational readiness assessments, supply chain risk management, and operation and maintenance activities.

5.3. Interoperability.

5.3.1. Cybersecurity products (e.g., firewalls, file integrity checkers, virus scanners, intrusion detection systems, anti-malware software) should operate in a net centric manner to enhance the exchange of data and shared security policies.

5.3.2. Semantic, technical, and policy interoperability will be used to integrate disparate cybersecurity products into a net centric enterprise that can work together to create new intelligence and make/implement decisions and network speed.

5.3.3. Semantic, technical, and policy interoperability support products that are designed to provide security for communication between different IT systems. Interoperable communications must be consistent with approved cryptographic design and current system implementation standards.

5.3.4. Standards-based approach. The cybersecurity and cyber space defense data strategy will enable semantic, technical, and policy interoperability through a standards-based approach that has been refined by many in the industry, academia, and government.

5.4. Cyberspace Defense

5.4.1. Cyberspace Defense uses architectures, cybersecurity, intelligence, counterintelligence, and other security programs to harden enterprise information technology to be more resistant to penetration and disruption. The goal is to also strengthen the company's ability to respond to unauthorized activity and defend corporate information systems and networks against sophisticated and agile cyber threats and to quickly recover from cyber incidents.

5.4.2. Defense of all corporate networks is under the direction of the CIO. Cyberspace Defense is integrated with other elements of network operations.

5.4.3. Continuous Monitoring Capability. The CIO shall establish and maintain a continuous monitoring capability that provides cohesive collection, transmission, storage, aggregation, and presentation of data that conveys current operational status to affected corporate stakeholders. The company will achieve cohesion using a common continuous monitoring framework, lexicon, and workflow as specified in NIST SP-800 – 137.

5.4.4. Penetration and Exploitation Testing. Evaluation of cybersecurity during an acquisition event must include independent threat representative penetration and exploitation testing and evaluation of the complete system cyberspace defenses including the controls and protections provided by computer network defense service providers. Penetration and exploitation testing must be planned and resourced as part of the validation test documentation process.

5.4.5. Insider Threats. It is understood that threats to business systems may come from within. Insider threats must be addressed in accordance with policies and procedures at the corporate level.

5.4.6. Users of corporate business systems shall be required to note and report any observed or suspected security weaknesses or threats to the appropriate manager/supervisor or the chief information officer. All users must report weaknesses as soon as possible. Users must not attempt under any circumstances to prove a suspected weakness as testing weaknesses could be perceived as a potential misuse of the system.

5.4.7. Procedures shall be established for reporting security software malfunctions. The following shall be considered:

5.4.8. The symptom of the problem and any messages appearing on the screen should be noted;

5.4.9. The computer must be isolated, if possible, and use of it stopped until the problem is resolved;

5.4.10. The matter should be reported immediately to the CIO/Director of Information Systems or designate for appropriate investigation.

5.5. Performance

5.5.1. <COMPANY NAME> shall implement processes and procedures to accommodate three conditions necessary to realize effective cybersecurity consistently implemented across the enterprise. These include the following:

5.5.2. Organization Direction. This includes organizational procedures for establishing and communicating priorities and objectives, principles, policies, standards, and performance measures.

5.5.3. A Culture of Accountability. This includes aligning internal processes, maintaining accountability, and informing, making, and following through on decisions with implications for cyberspace protection and cybersecurity.

5.5.4. Insight and oversight. This includes measuring, reviewing, verifying, monitoring, facilitating, and remediating to ensure coordinated and consistent cybersecurity implementation and reporting across all organizations without impeding normal business processes.

5.5.5. Cybersecurity Metrics. Strategic cybersecurity metrics will be defined, collected, and reported by the CIO in partnership with senior management. The CIO will develop an issue guidance regarding how cybersecurity metrics are determined, established, defined, collected, and reported.

5.6. Identity Assurance

5.6.1. Identity assurance ensures strong identification and authentication as well as eliminates anonymity in information systems so that access and access behavior are visible, traceable, and enable continuous monitoring for cybersecurity.

5.6.2. Person and non-person entity identity policies, standards, information, infrastructure, issuance, and revocation processes and procedures that bind physical and digital representation of entities will incorporate measures to ensure the integrity, authenticity, security, privacy, and availability of authoritative identity information access across the full spectrum of corporate information systems.

5.6.3. All corporate employees will use only corporate approved identity credentials to authenticate entities requesting access to or within the corporate information systems environment. This requirement extends to all external contractors as well.

5.6.4. The identification of all personnel and external contractors accessing corporate business systems must be fully documented to deny anonymity and deter abuse of authorized system access. The company will implement procedures to record, track, and monitor specific access to networks, applications, and Web servers.

5.6.5. Information and infrastructure that support identity reliant functions, processes, and procedures used in support of business operations, including but not limited to identity credentialing, will incorporate measures to ensure the confidentiality, integrity, authenticity, and availability of identity data or identity credentials.

5.7. Privileged Users (System Administrators)

5.7.1. All privileged users (system administrators) must:

5.7.2. Configure and operate IT within the authorities invested in them according to corporate cybersecurity policies and procedures.

5.7.3. Notify the responsible manager or director of any changes that might affect corporate security posture

5.8. Authorized Users

5.8.1. Authorized users must:

5.8.1.1. Immediately report all cybersecurity related events and potential threats and/or vulnerabilities to the appropriate supervisor or manager.

5.8.1.2. Protect authenticators commensurate with the classification or sensitivity of the information accessed and report any compromise or suspected compromise of an authenticator to the appropriate supervisor or manager. Protect pcs, terminals, workstations, or other input/output devices and resident data from unauthorized access.

5.8.1.3. Inform each supervisor and/or manager when access to a system is no longer required (e.g., completion of a project, transfer, retirement, or resignation)

5.8.1.4. Observe policies and procedures governing the secure operation and authorized use of all corporate IT systems in accordance with internal policies.

5.8.1.5. Use corporate business systems for official or authorized purposes only.

5.8.1.6. Not unilaterally bypass, strain, or test cybersecurity mechanisms. If cybersecurity mechanisms must be bypassed, users shall coordinate the procedure with his/her immediate supervisor and receive written approval from senior management.

5.8.1.7. Not introduce or use software, firmware, or hardware that has not been approved by his/her immediate supervisor and designated representative from the IT department.

5.8.1.8. Not relocate or change IT equipment or network conductivity without proper authorization.

5.8.1.9. Meet minimum cybersecurity awareness requirements in accordance with this procedure.

5.9. Cybersecurity Training

5.9.1. It is the goal of to develop and maintain a trained and qualified cybersecurity workforce by providing a continuum of learning from basic literacy to advance skills, recruiting and retaining highly qualified professionals, and keeping workforce capabilities current in the face of constant change. The following policies apply with respect to cybersecurity workforce training.

5.9.2. All cybersecurity personnel must be assigned in writing to identified cybersecurity positions and trained in accordance with corporate policy.

5.9.3. All authorized users of corporate business systems must receive initial cybersecurity awareness orientation as a condition of access and, thereafter, participate in the corporate enterprise cybersecurity awareness program.

5.9.4. Cybersecurity functions that may be performed by contractors or non-employees will be specifically identified.

6. References

6.1. 21 CFR, Part 11, Electronic Records
6.2. 21 CFR, Section 820.40, Document Controls
6.3. ISO 9001Document Requirements
6.4. ISO 13485, Document Requirements
6.5. QA-008 Documentation Control

7. Revision History

Rev #	Date	Change
1		New Document

8. Attachments - none