PO 3.01.01 - Information Security and Privacy Policy

Information is an asset which, like any other asset owned by Company, has significant value. Information security is a critical component to ensure the confidentiality, integrity and availability of information. This policy has been developed to establish the minimum requirements that are necessary to protect information assets against unauthorized access, modification or destruction for both physical and network security.

Scope:

The Policy pertains to all types of information resources, including:
(1) Hardcopy data printed or written on paper
(2) Data stored electronically
(3) Communications sent by mail, courier or transmitted electronically
(4) Removable Media including but not limited to information stored on tape, CD/DVD, video, and USB flash drive.
(5) Recorded audio

PR 3.01.01(a) - Designate Reviewer of Information Security and Privacy Policy

The Company has appointed individual(s) to review and make recommendations for changes to the Information Security and Privacy Policy. This individual is responsible for coordinating and overseeing the Information Security and Privacy Policy.

PR 3.01.01(b) - Management Approval of Information Security and Privacy Policy

On an annual basis or as necessary based on a change in operations, legal and regulatory requirements, industry best practices, and available technology, management reviews, updates and approves the Information Security and Privacy policy. If exceptions to the Information Security and Privacy Policy are necessary, that request is evaluated by the individual responsible for the Policy. Approved exceptions will be documented and recorded.

PR 3.01.01(c) – Distribution of Information Security and Privacy Policy

Upon approval, management distributes Policy to Applicable Parties to acknowledge receipt. Policy delivery and acknowledgement is maintained on the Tracking Log.

PR 3.01.01(d) - Background Checks for Employees

At hire, a background check will be performed for all employees who have access to NPI, unless prohibited by law.
(1) Order background check.
(2) Background check results are reviewed and then approved or denied by management.
(3) Place evidence (invoice/documentation) in a single location such as the employee file.

PR 3.01.01(e) - Background Checks for Service Providers

The Company obtains and stores proof that a background check has been performed for all Service Providers that have access to NPI or Company information systems.

PO 3.01.02 - Clean Desk Policy

The Company maintains a Clean Desk Policy to reduce the threat of a security incident to NPI.

PR 3.01.02(a) – Clean Desk Procedure

All Applicable Parties must:

(1) Close paper and/or electronic files containing NPI when they are away from their desk.
(2) Log-off or lock their computers when unattended.
(3) At the end of each working day, safeguard all documents, files, portable devices, and electronic media containing NPI in a locked desk, file cabinet, or secure location.
(4) Store materials (e.g. day planners) with NPI in a locked drawer or take them when away from desk for extended periods of time, including overnight.
(5) Secure all keys used to access NPI.
(6) Remove all documents from copy and facsimile containing NPI
(7) Secure passwords at all times.

Management periodically checks to ensure compliance with the procedure.

PO 3.02.01 – Risk Identification and Assessment Policy

The Company has established an Information Security Risk Assessment that ranks risks including locations, systems, and methods for storing, processing, transmitting, and disposing of NPI.

PR 3.02.01(a) – Risk Identification and Assessment Procedures

Risk Evaluation and Implementation of Controls:
(1) Identify and prioritize risks associated with the protection of NPI. These risks are evaluated by:
(a.) The impact and likelihood of an occurrence
(b.) Estimated costs and impact if an event actually occurred
(c.) Evaluation of the priority based on the impact, likelihood, costs and other important factors
(d.) Location of NPI (onsite and offsite)
(e.) Access by Applicable Parties
(2) Implement controls to mitigate risks where appropriate (e.g. firewall, encrypted USB flash drive, implementing patches or software fixes).

Risk Assessment Testing:
(1) Risk Assessment is tested annually by an internal or external resource.
(2) Track any exceptions and/or control gaps on Risk Assessment Worksheet.
(3) Management evaluates and responds to the Risk Assessment Worksheet including timeframe for remediation.

Risk Assessment Remediation:
Exceptions and/or control gaps are remediated by one of the following methods:
(1) Reduce or eliminate the risk.
(2) Changes are made to procedures as applicable based on the risks perceived, scope and types of activities, and access to NPI.
(3) Obtain documented approval from Management whenever the Company deviates from Information Security and Privacy Policy.

Document completion of remediated items on the Risk Assessment Worksheet.

Risk Assessment Review:
Annually a review includes, but is not limited to, information systems, including network and software design; information processing, storage and disposal; detecting, preventing and responding to attacks, intrusions or other system failures.

PO 3.03.01 – Employee Training, Management, and Responsibilities Policy

The Company provides management and training for Applicable Parties to help ensure compliance with the Information Security and Privacy Policy.

PR 3.03.01(a) – Employee Training

At hire and annually, the Information Security and Privacy Policy is emphasized through training to Applicable Parties of their responsibilities for handling, protecting and destruction of NPI. This training includes, but is not limited to the Acceptable Use of Information Technology Policy, Information Security and Privacy Policy, and Record Retention and Disposal Policy.

PR 3.03.01(b) – Violations: Reporting and Penalties

Applicable Parties are required to report (perceived or actual) violations of the Information Security and Privacy Policy to the designated Company individual.

Violation of the Information Security and Privacy Policy may result in disciplinary action, up to and including termination.

PO 3.04.01 – Information Security Policy

All information stored, handled or processed by the Company is protected by controls appropriate for the associated level of risk and impact.

PR 3.04.01(a) – Information Security Procedure

Appropriate level of controls over all information stored, handled or processed by the Company is managed as follows:
(1) Assign an "owner" to all information. An "owner" is a party that is responsible for its security while the information is being stored, handled or processed by the Company.
(2) Categorize the information.

All information will be classified into one of the following categories:
(1) Public – information generally available (e.g. brochures, job openings, press releases)
(2) Internal Use Only – information for Company employees (e.g. internal email messages, company intranet, internal policy/procedure, training materials, employee performance evaluations, customer transaction data, computer passwords, company financials).
(3) NPI – Non-public Personal Information is any data or information considered to be personal in nature and not subject to public availability as defined by the Gramm-Leach-Bliley Act ("GLB Act") of 1999

Information and records designated as Internal Use Only or NPI must be labeled in some fashion that makes users aware of the sensitivity of that information. There are various forms of "labeling" or "tagging" and some examples include:
(1) Identifying the classification in the header, footer, or cover page of a document;
(2) Displaying the classification during a system login screen;
(3) Labeling folders;
(4) Putting signs on cabinets that contain sensitive records; and
(5) Using an applicable ink stamp on the document.

PR 3.04.01(b) – Logical Access

Onsite and offsite Logical Access:
(1) Each Applicable Party is required to have a unique User ID and password which is not shared. The User ID will be permanently decommissioned when no longer required.
(2) Passwords must follow the Company's Password Controls.
(3) Identify appropriate access level based on job role and responsibility on Role & Responsibility Checklist.
(4) Identify appropriate access level based on business need.
(5) The individual responsible for the Policy reviews access level when job roles and responsibilities and/or business needs change, with more frequent reviews occurring for those with privileged access rights.

Segregation of Duty Note: Individuals with the ability to add, modify and remove user access are not assigned to perform business transactions within the system.

PR 3.04.01(c) – Physical Security Controls

The Company incorporates all contractual and legal requirements based on local, state and federal law into the physical security controls for every location where NPI is stored or other restricted areas. Review of controls is conducted at least annually.

(1) The Company uses secure points of entry into buildings and any interior offices where NPI is stored or other restricted areas, and requires the use of either keys, individual access codes or personal keys/fobs.
(2) As applicable, physical access to data center, server room or offsite storage will be granted according to the employee's role, level of access necessary to perform duties associated with the role, and in accordance with the data category (Public, Internal Use Only, NPI).
(3) Company equipment and devices, keys/fobs, material, hardware and software, Removable Media and any documents will be returned upon termination of employment or contract. User accounts and network access including remote access will be immediately disabled for terminated Applicable Parties.

PR 3.04.01(d) – Network Security Controls

The Company incorporates all contractual and legal requirements based on local, state and federal law into the network security controls where NPI is stored. Review of controls is conducted at least annually.

(1) Security controls (e.g. password protection, encryption) for physical media, electronic media (e.g. email, database access) and wireless devices are used to prevent unauthorized access, misuse, or corruption of NPI while in transit.
(2) The Company's network systems (e.g. firewall) are configured to detect and log intrusion events, and alert appropriate individuals.
(3) Backups are made and maintained for all critical systems and data.
(4) Company systems are configured to record the User ID of persons who access the system.
(5) Anti-virus software is installed, functioning and maintained on servers, users workstations, and laptops. Anti-virus is configured to scan external media as applicable.
(6) Applicable Parties other than system administrators are not permitted to disable anti-virus software.
(7) Remote access (e.g. Virtual Private Network, "VPN") requires authentication to Company networks based on job roles and responsibilities and business need.
(8) The Company maintains security authentication (e.g. password, access token) to secure computers and other office equipment that contains NPI.

PR 3.04.01(e) – Password Controls

(1) Access system requires passwords that are at least six or more alphanumeric and special characters, and do not contain common words, User ID, first or last name.
(2) Applicable Parties are required to change their password after initial assignment and regularly thereafter based on the Company applicable password standards.
(3) When resetting password, new password cannot match prior six passwords.
(4) Applicable parties are required to report any instance of compromised passwords and to change possibly compromised passwords immediately.

PR 3.04.01(f) – Restricting use of Removable Media with NPI

(1) Removable Media containing NPI is not permitted without prior written approval from the individual responsible for the Policy.
(2) Upon such approval, it is the individual's responsibility to protect the Removable Media in their possession from theft or unauthorized access. Security controls (e.g. password protection, encryption) for Removable Media are used to prevent unauthorized

access, misuse, or corruption of NPI while in transit.
(3) Applicable Parties are instructed not to leave documents, Removable Media containing NPI in a location (unlocked vehicle, hotel room) accessible to others.

PO 3.04.02 – Acceptable Use of Information Technology Policy

The Company established an Acceptable Use of Information Technology Policy that describes acceptable use of Company assets and systems, including but not limited to use of Internet, email, and equipment. The Company has the right to monitor networks, computer systems, internet usage and email for Applicable Parties to confirm compliance with the Policy.

PR 3.04.02(a) – Acceptable Use of Information Technology Procedure

(1) Internet access is provided as necessary to perform the job assigned to the Applicable Party. If an Applicable Party needs additional access, a request is directed to the manager, who must approve the access.
(2) The Company reserves the right to remove any Internet posting by an Applicable Party that is deemed inappropriate and/or damaging to the Company's reputation.
(3) Applicable Parties are not permitted to install, download or remove software without prior approval from management.

PO 3.04.03 – Customer Privacy Policy

The Company collects NPI from the following sources:

(1) Information received from customers on applications or other forms.
(2) Information about customer transactions with the Company, its affiliates, or others.
(3) Information received from a consumer reporting agency.

The Company restricts access to NPI to those Applicable Parties who need to know that information to provide products or services to customers. The Company maintains physical, electronic, and procedural safeguards that comply with federal regulations to guard NPI.

PR 3.04.03(a) – Designate Reviewer of Customer Privacy Policy

The Company appoints an individual(s) to review and make recommendations for changes to the Customer Privacy Policy.

PR 3.04.03(b) – Management Approval of Customer Privacy Policy

On an annual basis or as necessary based on change in operations, legal and regulatory requirements, industry best practices, and available technology, management reviews, updates and approves the Customer Privacy Policy. If exceptions to the Policy are necessary, that request will be evaluated by the individual responsible for the Customer Privacy Policy. Any approved exceptions will be documented and recorded.

PR 3.04.03(c) – Provide Customer Privacy Policy

The Company provides the Customer Privacy Policy to its customers as required by law. Proof of notification to customer is retained by the Company. The Customer Privacy Policy is accessible by customers through the Company website if applicable.

PO 3.05.01 – Record Retention and Disposal Policy

The Company maintains a Record Retention and Disposal Schedule based on the classification of information (Public, Internal Use Only, NPI) and all legal and contractual requirements along with applicable industry standards. Data classified as Public is excluded from retention unless deemed necessary by management.

PR 3.05.01(a) – Record Retention and Disposal Procedure

Company Record Retention and Disposal:
(1) Designate retention time frames or destroy-by-dates for each classification of information.
(2) Information is physically destroyed or securely overwritten when no longer needed.
(3) Media and data will be destroyed by performing the following:
(a) If physical media: cross-cut shredding or incineration.
(b) If electronic: render data on electronic media unrecoverable by securely wiping, purging, degaussing, or physically destroying (such as grinding or shredding hard disks). This paragraph applies to rental equipment and other equipment not Company owned when it is returned to owner (e.g. leased copy machine).

Vendor Record Retention and Disposal:
(1) Maintain contract agreements, service level agreements (SLAs), and any disposal certificates as applicable.

PO 3.06.01 – Overseeing Service Providers Policy

The Company takes reasonable steps to select and retain service providers that are capable of appropriately safeguarding NPI.

PR 3.06.01(a) – Overseeing Service Providers Procedure

(1) Select - Prior to selection of Service Providers, due diligence will be required such as an evaluation of their security policies, background screening on staff, financial viability, insurance coverages, references and disaster recovery plans. Due diligence materials are retained.

(2) Verify- The contract provisions, service level agreements and non-disclosure agreements between the Company and the Service Providers will be in accordance with the Company's Information Security and Privacy Policy. The contract and agreements provide appropriate remedies for violations.

(3) Implement- Service Providers will implement appropriate security controls in accordance with the objectives of the Company's Information Security and Privacy Policy.

(4) Monitor - Where Service Providers are subject to expanded safeguards as applicable by regulatory, legislative or contractual obligations, the Company will monitor those expanded safeguards.
(a) The Company designates an employee as the Service Provider contact.
(b) The Company Service Provider contact monitors performance on a regular basis.
(c) If contract provisions, service level agreements or non-disclosure agreements are violated, the Company Service Provider contact takes appropriate action.

PO 3.07.01 – Data Breach Incident Reporting Policy

The Company monitors, investigates attacks/intrusions, and responds to Data Breach incidents.

PR 3.07.01(a) – Data Breach Incident Reporting Procedure

The Company has designated a responsible individual as the Data Breach contact for implementing this procedure.

(1) Monitor:
(a) Deviation from policies, procedures or misuse of information and information systems will be monitored.
(a) All breaches of information security or loss of any device, actual or suspected, must be reported and will be investigated by the Data Breach contact.
(b) To the extent monitoring is being conducted by a Service Provider, Service Provider shall agree to follow Data Breach Incident procedure.

(2) Investigate:
(a) Data Breach contact determines impact of incident.
(b) Data Breach contact analyzes and preserves log information.

(3) Respond:
(a) Data Breach contact notifies Company management
(b) Customers and law enforcement will be notified of any Data Breach in accordance with applicable legal and regulatory requirements and the Customer Privacy Policy.

(4) Process Improvement & Remediate:
(a) System and processes are updated to prevent further intrusion as applicable.
(b) Any delays in breach notifications will be documented by the Data Breach contact.
(c) Execute remediation as applicable (e.g. employee access restricted).
(d) Disciplinary action against Applicable Parties will be taken as appropriate.

PO 3.08.01 – Business Continuity and Disaster Recovery Policy

A Business Continuity and Disaster Recovery plan is in place to protect critical business processes from effects of failures or disasters. This plan ensures secure methods to protect Company information and the timely resumption of business information systems.

PR 3.08.01(a) – Business Continuity and Disaster Recovery Procedure

(1) Identify and prioritize critical business components.
(a) Physical Offices
(b) Equipment
(c) Applications and services
(d) Network
(e) Telecom
(f) Loss of critical Service Providers

(2) Identify risks to critical business components.
(a) Environmental (e.g. fire, flood, storm)
(b) Technological (e.g. hard drive failure, loss of internet)
(c) Vandalism (e.g. malicious computer attack)

(3) Identify timely restoration and alternative workarounds for each critical business components.
(a) Scheduled tasks to be completed
(b) Owner of scheduled tasks
(c) Application and services to be recovered

(4) Identify individuals to institute workaround including contact information.

(5) Backups are made and maintained for all data including offsite and secure locations.

(6) Recovery of systems and data must be tested periodically to ensure that processes and procedures are effective.

(7) Results of testing are documented on the Tracking Log.

(8) Copy of Business Continuity and Disaster Recovery Plan is distributed to all individuals who require them in case of emergency.