POLICY			
Policy Name	ISO Information Security Policy		
Policy Number	ISO-P022	**Version Number**	5.0
Supersedes Policy	N/A	**Effective Date**	9/4/2019
Last Reviewed Date	3/15/2023	**Last Revised Date**	10/19/2020
Policy Owner		**Approved By**	
Name	David Christensen	**Name**	Srinivasan Venkatramani
Title	CISO	**Title**	CTPO
Date Approved	3/15/2023	**Date Approved**	3/15/2023

Objective

This policy has been developed to achieve the following objectives as outlined in the Security Program Charter:

- Identify and address security and compliance risks within a period of up to one year unless a remediation treatment plan extension is granted.
- Meet the regulatory requirements of governing bodies for privacy, security, and other applicable laws and regulations.
- Provide ongoing risk and cybersecurity communications that is transparent and seamless among all stakeholders.
- Ability to respond to cybersecurity incidents internal and/or external that are acts or attempts, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse a Licensee's electronic systems or information stored on such systems.
- Reduce the likelihood of a catastrophic cybersecurity incident materializing and causing irreparable harm to PlanSource and its business operations.

Responsibilities

Business Owner - This is the department manager or the Product manager accountable for the systems and related services within their assigned business unit.

Change Review Board (CRB) - The Change Review Board oversees change procedures, validates and approves documented changes. The CRB also reviews and approves significant, major and high impact system changes. The CRB reviews the information provided in the RFC to ensure the changes are sufficiently researched, documented, planned, and executed.

Chief Information Security Officer (CISO) - The CISO is the overall owner of this policy and will ensure it is maintained and updated accordingly. Corporate Risk and IT Compliance will ensure compliance audits are accomplished to validate compliance with this policy.

Compliance - This team ensures that PlanSource Personnel observe PlanSource policies and procedures. This team also engages third party business partners to certify that PlanSource products meet appropriate certifications and regulatory requirements.

Designated Owner - This is a business unit or business role. The business entity or assigned individual has primary responsibility for the assets assigned to them, whether in their custody or in the custody of others. Designated owners may delegate routine tasks associated with the assets or systems under their supervision. Owners are responsible for ensuring the asset is correctly classified, for the day to day maintenance of identified controls, that access controls are defined and periodically reviewed, and vulnerabilities are identified and patched. Software assets are assigned a designated owner who is a trained system administrator.

Human Resources - The HR team is the Information Owner for personnel data and is responsible for asserting the security and privacy rules to protect that data. This team distributes HR-related information to PlanSource Personnel and manages the onboarding of new personnel and updating of personnel who terminate or change responsibilities with PlanSource.

Incident Response - The IRT is responsible for managing the successful resolution of Team security incidents or security breaches reported by PlanSource Personnel. The IRT has full authority to take whatever action is deemed necessary to resolve an incident or breach in order to return the PlanSource business to normal productivity as quickly as possible.

PlanSource Managers - PlanSource Managers are responsible to ensure their staff is aware of and compliant with the policies, procedures, and practices that apply to their business units. PlanSource Managers are also responsible for filing policy exceptions with Information Security, reporting policy violations, and implementing plans to become compliant with new and revised policies and standards.

PlanSource Personnel - PlanSource Personnel are inclusive of all categories of workers. They are responsible for protecting the information and devices under their control, understanding and complying with PlanSource's Information Security policies, and reporting any suspicious system activity to management and Information Security.

Information Custodian - Custodians are in physical (or logical) possession of information and/or information systems. Custodians are specifically designated for different types of information. They follow the instructions of the Information Owners and/or operate systems on behalf of the Information Owners, but also serve users authorized by the Information Owners.

Custodians define information systems architectures and provide technical consulting assistance to the Information Owners so systems can be deployed to meet business objectives. If requested, Custodians provide reports to the Information Owners concerning system operations, information security problems, etc.

Custodians safeguard the information in their possession, including implementing access control systems to prevent inappropriate disclosure, as well as developing, documenting, and testing system contingency plans.

Information Owner - This is an individual, organization, or entity that determines the value and classification of the data and associated system(s) assigned to them and provides appropriate disclosure, distribution, and protection requirements. The Information Owner has primary responsibility for the information assigned to them whether it is in their custody or in the custody of others. As such, they must:

- Authorize the use of the data that is consistent with its intended purpose;
- Protect aggregate data adequately. At minimum, assign the highest classification of any data component and consider if the collective data requires a higher classification;
- Protect data from unauthorized use, access, disclosure, alteration, or disposal;
- Ensure a scalable backup system is fully-functional in order to prevent the loss of business-critical information; and
- Report unauthorized use, access, or disclosure of data to the applicable organization.

Information Security (IS) - The Information Security team (InfoSec) manages the development, maintenance and enforcement of information security policies and standards, in accordance with generally accepted best practices, focusing on business and risk objectives.

Information Technology (IT) - Implements access controls and monitors the availability of the information assets, in accordance with regulatory constraints and the instructions of Information Owners.

IT Operations (IT Ops) - IT Operations is responsible for analyzing and prioritizing the results/vulnerabilities and communicating those results to appropriate teams for remediation.

IT Owner - This is the Information Technology person accountable for each system or service. For internal services this is someone in ESS and for ICHS this is someone in the Cloud Trust organization.

Legal - As it related to the Information Security function, the Legal team reviews policies and procedures to ensure that they are consistent with relevant laws and regulations. They provide legal advice to other teams and vulnerabilities are identified and patched. Software assets are assigned a designated owner who is a trained system administrator.

Network Administrators - Network Administrators manage access to and maintain functionality within PlanSource's network environment.

Relationship Owner - This is an individual or organization responsible for managing the business relationship between PlanSource and an external third-party.

Security Administrators - Designated Security Administrators include operational functional teams such as systems administrators, database administrators, and network administrators. These functional teams maintain the responsibility for the management of security controls and configurations within the information systems they support. They implement security mechanisms and maintain the requisite technical expertise to support them. They ensure systems and services comply with approved information security policies, mandatory standards/baselines, and recommended guidelines and procedures.

Development Team – Development teams are responsible for designing, developing and testing PlanSource software products. Each Development team is responsible for implementing the secure software development lifecycle and all aspects of this policy as part of every system development and/or maintenance project.

System Administrator - The SA manages access to applications and systems on behalf of the System Owner.

System Operator - System Operators run and maintain applications and systems.

System Owner - The System Owner manages system upgrades and patches, while collaborating with IT Operations on continuous administration of the system.

Table of Contents (if applicable)

Definitions

Account ID-There are three different types of Account IDs:

- Individual Account IDs (aka User Accounts) are assigned to PlanSource Personnel in order to access PlanSource Information Systems to perform their daily work activities. Individual accounts are assigned to personnel for their exclusive use; personnel must not to share them with others.
- System Administrator IDs (aka System Admin Accounts) are assigned to PlanSource Personnel who manage and maintain PlanSource computer systems and networks. These Account IDs can be assigned individually, not to be shared with others; or as a Shared Account ID where two or more System Administrators use the Account to maintain PlanSource systems.
- System Accounts (aka Sys Account) are assigned to scripts and other forms of automation, and typically have limited privileges to implement specific controls or functions. Other System Accounts are reserved for emergencies (e.g. “break glass passwords”) and have privileged access. PlanSource Personnel must not use these credentials as part of their normal job function, and their credentials must be protected from misuse by storing and managing them only in IT-sanctioned credential management systems.

Advanced Encryption Standard- AES is a specification for the encryption of electronic data established in 2001 by the National Institute of Standards and Technology (NIST).

Anti-virus Software - Anti-virus software was originally developed to detect and remove computer viruses, hence the name. However, with the proliferation of other kinds of malware, anti-virus software started to provide protection from other computer threats. In particular, modern anti-virus software can protect from: malicious Browser Helper Objects (BHOs), browser hijackers, ransom ware, key loggers, etc.

Authorization Decision Assertion - This is a request to grant or deny a PlanSource Personnel access a specified resource.

Bug/Defect Patch - This type of patch addresses an issue or defect related to the general functionality of a PlanSource system.

Business-critical Information -This is information deemed necessary for PlanSource to continue operations in the event of a disaster. PlanSource’s management in conjunction with the Information Owner determines whether information is deemed “business-critical”. Information of this type includes, but is not limited to, product and engineering data, financial information, HR data, IT systems and applications.

Business Information - Business information is considered any information about the business that is private or confidential in nature. The loss of which would be detrimental to the success of the business. For example, financial records, stockholder information, account IDs, business strategy, credit information, product research, formulas, etc.

Candidates - Individuals being considered for employment, consulting or contracting positions.

Change in Contract - A contract is a legally binding agreement between PlanSource and another party, typically a third party vendor or contractor (aka “the other party”). It is a written document outlining the duties and benefits prescribed to PlanSource and the other party. A contract modification occurs when both parties agree to change any of the terms in the original agreement. A contract can be modified in whole or in part, depending on the needs of PlanSource or the other party. A contract can be modified either before signing or after the contract is formally agreed to.

For any contract modification to be considered valid, both PlanSource and the other party must agree to the subsequent changes. If either party does not agree to a contract modification, the changes are usually not enforceable. Valid modifications will be enforced and are binding according to contract law. Contract modification can occur for a variety of reasons including:

- Extending or terminating the contract
- Modifying the contract's duration
- Altering the quantity of items required under the contract
- Adding or subtracting any goods or services in the contract
- Changing terms such as payment, delivery, or receipt of products or services

A contract might also need to be modified for other reasons besides the desires of PlanSource and the other party. For example, contract modification might be necessary due to a statutory requirement. Or, a legal judgment might necessitate a modification to a contract.

Only PlanSource contracting officers, acting within the scope of their authority, are empowered to execute contract modifications on behalf of PlanSource.

Administrative Change - is a unilateral contract change in writing that does not affect the substantive rights of PlanSource or the other party.

Change Order- means a written order, signed by the PlanSource contracting officer, directing the other party to make a change that the Change clause authorizes PlanSource to order without the other party's consent.

Contract modification - is any written change in the terms of the contract.

Bilateral modification - is a change to the contract signed by the other party and the PlanSource contracting officer on behalf of PlanSource. This type of modification includes:

- Making negotiated equitable adjustments resulting from issuing a Change Order
- Reflecting other agreements between the parties modifying the terms of the contract

Unilateral modifications - are a change signed only by the PlanSource contracting officer. This type of modification includes:

- Administrative changes
- Issuing a Change Order
- Making changes authorized by clauses in the contract other than the change clause.
- Issue a termination notice

Change Management (CM) - The process that controls the lifecycle of changes made to PlanSource information systems. Change Management is the process of documenting a change, reviewing the potential impact of the change, controlling the timing of the change and, verifying the completeness of the change. The CM process ensures changes are recorded, evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.

Change Management System - The software system that centrally tracks, manages workflow and records the status of Request for Change (RFC) tickets.

Change Manager - The Change Manager provides overall direction for and enforcement of change policies and processes. The Change Manager ensures the change management process is uniform, consistent, and followed throughout the managed environment. While the Change Management process provides the mechanism for approving (or denying), proposed changes, the final decision authority for approving changes lies with the Change Manager. In order to make sound decisions, the Change Manager relies on input from the CRB.

Change Requestor - The Change Requestor is responsible for initiating the change and managing it through its lifecycle. This includes working with stakeholders to address any issues and ensuring the RFC is approved prior to CRB review. The Change Requester serves in a communications role, and therefore assumes responsibility for customer communications.

Change Review Board (CRB) - This committee assists the Change Manager in the assessment, prioritization, authorization and scheduling of changes. The CRB is the final authority to ensure the Change Management process

meets its objectives. This board has representatives from various IT teams and may include representatives from the Business and third party suppliers.

Change Schedule - Contains details of approved changes for a pre-defined time period.

Computer Virus - A computer virus is a malware program when executed replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive. When this replication succeeds, the affected areas are said to be "infected".

Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging keystrokes.

Configuration Item (CI) - A Configuration Item (CI) is any component that needs to be managed in order to deliver an IT service. CIs may be comprised of hardware, software or documentation. Examples include services, servers, environments, equipment, network components, desktops, mobile units, applications, licenses, telecommunication services and facilities.

Information about each CI is recorded in a Configuration Record within the Configuration Management System and is maintained throughout its lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT services, hardware, software, buildings, people, formal process documentation and Service Level Agreements (SLA).

Configuration - The CMDB is the database that contains relevant information about the Management Database components in the IT environment. Configuration Management is responsible for identification and labeling of the CIs including their respective owner and relationships between them. For the purposes of Change Management, the CMDB identifies relationships between an item to be changed and any other component of the infrastructure.

Controls - A method of managing risk (including policies, procedures, guidelines, practices or organizational structures), which can be of an administrative, technical, management, or legal nature.

Coordinated Universal Time - “UTC” (from the French “temps universel coordonné”) is the primary time standard by which the world regulates clocks and time. It is a closely related successor to Greenwich Mean Time (GMT). UTC is based on International Atomic Time with leap seconds added at irregular intervals to compensate for the slowing of Earth’s rotation. Leap seconds keep UTC within 0.9 second of universal time.

Customer Private Information (CPI) - This is any personal or private information about a customer, business partner, vendor, or other entity conducting business with PlanSource and customer sourced information.

Device - Typically, this is any hand-held mobile computing or communication device (e.g. smart phones, notebooks, laptops, tablets, etc.) capable of accessing a computer network without being physically tethered to the environment

Emergency Change - This is a change that requires circumvention of the normal change management cycle in order to address an immediate and critical need, when service must be restored as soon as possible. Only changes that need to be implemented as soon as possible to address a service failure or potential service failure are considered Emergency Changes.

Emergency Changes will be generated from high-priority problem tickets and have adequate business justification and authorization

Encryption - Encryption is the process of encoding messages or information in such a way that only authorized systems or individuals can read it.

Full Access VPN - This is a type of connection which assigns an IP address to the client in order for that client to access a full range of resources on the PlanSource network.

Guidelines - Recommended actions and/or industry best practices designed to clarify activities supporting the enforcement of policies.

Hash - Hash is any encryption-type function that can be used to map digital data of arbitrary size to digital data of fixed size, with slight differences in input data producing very big differences in output data. Functions have many information security applications, notably in digital signatures, message authentication codes, and other forms of authentication. Hash can also be used as ordinary functions, to index data in hash tables, fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption.

Hash–based MAC (Message Authentication Code) - HMAC is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authentication of a message.

High Priority Change - A high priority change is a normal or standard change that has a significant impact (see Significant Change) which requires that it be prioritized ahead of other change requests in the same Change Schedule.

HIPAA - The Health Insurance Portability and Accountability Act, was enacted by the US Congress in 1996. Title I protect health insurance coverage for workers and their families when they change or lose their jobs. Title II, known as the Administrative Simplification provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

Immediately - "Immediately" is an arbitrary term that can mean different time-frames for different situations. For example:

- "Immediately disconnect system access upon termination" could mean the user access to PlanSource network should be removed within 24-hours after termination.
- "Immediately terminate system access for someone being escorted from the premises" could mean user access to PlanSource's network should be removed within an hour.

It is the responsibility of HR, IT, Legal and Corporate management to determine the time-frame associated with the term "immediately", given the circumstances of the situation.

Incident Response Team - The IRT is comprised of PlanSource Personnel trained in managing incidents that occur which have an impact on PlanSource's business continuity. This team will identify the severity of the incident and perform the activities needed to resolve the situation and make recommendations to eliminate a future reoccurrence of the incident.

PlanSource Personnel - Any PlanSource employee, partner, consultant, contractor, agent, vendor, distributor, or contractor who uses or is granted access to PlanSource facilities or information systems.

Information Assets - These are assets that consist primarily of databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational and support procedures, business continuity plans, fallback arrangements, audit trails, and archived data.

Information assets also include the physical assets, services, resources, software and intangibles that support the proliferation of information within the PlanSource global enterprise.

- Software Assets: application software, system software, development tools, and utilities;
- Physical Assets: facilities, computer equipment, communications equipment, removable media, and other equipment;
- Services: computing, communications services and general utilities;
- Personnel: personal qualifications, skills and experience; Intangibles: the reputation and image of PlanSource.

Information Processing Facility - Any physical location or device (e.g. datacenter, back-up location, third-party processing center, laptop, personal computer, server, network device, etc.) that manages (or processes) information assets owned or controlled by PlanSource. These facilities may be owned or operated by PlanSource, or business partners working on behalf of PlanSource.

Information Security – A Team dedicated to protecting data and other assets within PlanSource.

Event - a possible breach of information security or failure of safeguards, or a previously unknown situation that may threaten the security of PlanSource data.

Information Security Incident - A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening the security of data within PlanSource to include incidents like DDOS attacks.

Information System - This is any computer system or application that processes, maintains or stores information used by PlanSource to manage its global enterprise.

Information User - An Information User is any PlanSource Personnel who uses or processes PlanSource's information assets.

IT Service Management (ITSM) - This is a process-based practice intended to align the delivery of IT services with PlanSource needs, emphasizing benefits to customers. ITSM focuses on the delivery of end-to-end services using best practice process models. ITSM unifies service desk, incident, problem, change, asset life cycle, and service level management applications with a single CMDB, data model, workflow platform, and user interface.

Key - A "Key" in cryptography is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher. Without a key, the algorithm would produce no useful result. In encryption, a key specifies the particular transformation of plain text into cipher text, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes.

Least Privileged Access - The principle of least privilege (also known as the principle of minimal privilege or the principle of least authority) requires that in a particular abstraction layer of a computing environment, every module (such as a process, a user or a program depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose.

When applied to users, the terms least user access or least-privileged user account (LUA) are also used, referring to the concept that user accounts should run and also launch applications with as few privileges as possible. Software bugs may be exposed when applications do not work correctly without elevated privileges.

Logon Banner - A message, approved by IT and Legal, to which users must attest, that contains information related to expectation of privacy and acceptable use.

Major Change - Major changes potentially affect the department or entire company. They may affect multiple systems or applications. This type of change could involve high risk and/or potential impact to the Business. Multiple IT departments and multiple business sites may need to be notified.

Message Authentication Code MAC - is a short piece of information used to authenticate a message and to provide integrity and authenticity assurances on the message.

Integrity - assurances detect accidental and intentional message changes, while authenticity assurances affirm the message's origin.

Minor Change - Minor changes affect only a few users or systems. For example, application of a patch to fewer than 10 desktops or to one server, or the installation of a new printer.

Mobile Device - This can be any hand-held computing or communication device (e.g. smart phones, notebooks, laptops, tablets, etc.) capable of accessing a computer network without being physically tethered to the environment.

Non-Disclosure - An "NDA" is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to Agreement (NDA) share with one another for certain purposes but wish to restrict access to or by third parties. It is a contract through which the parties agree not to disclose information covered by the agreement. An NDA creates a confidential relationship between the parties to protect any type of confidential and proprietary information or trade secrets. As such, an NDA protects nonpublic business information.

Normal Change - This is a change that is not an emergency change or a standard change. This change goes through the regular CM process and is divided into three subcategories (minor, significant, major), which are evaluated according to the impact, risks and costs of change on the infrastructure.

Password - A password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which should be kept secret from those not allowed access.

Personally Identifiable Information (PII) - PII is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. PII can be any information about an individual including information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.

Policy - A principle or rule to guide decisions designed to achieve rational outcomes. A policy is comprised of an overarching statement, globally enforceable, and create possessing a reference of understanding. It contains and overarching statement and organizational principles identifying formal expectations related to what needs to be done

to manage protect and use assets. how assets are managed, protected and used. It establishes decisions, directions and precedents that act as a reference for decisions.

Policy Repository - A central location, usually on a company's intranet, designated as the official storehouse for security policies, procedures, guidelines and standards.

Related Policies or Standard Operating Procedures (if applicable)

- Systems Access Policy
- Remote Access Policy
- Security Risk Management Policy
- Business Continuity and Disaster Recovery Policy
- Configuration Management Policy
- Data Retention and Disposal Policy – Benefit System
- Compliance Policy
- Physical and Environmental Security Policy
- Data Classification Policy
- Systems Development Lifecycle Security Policy
- Production Access Policy
- Password Policy
- Monitoring and Logging Policy
- Mobile Device Security Policy
- Infrastructure Security Policy
- Third Party Risk Management Policy
- Clear Desk Clear Screen Policy
- Backup Policy
- Asset Management Policy
- Anti-Virus Malware Policy
- Acceptable Use Policy
- Cyber Security Incident Management Policy
- Cryptographic and Key Management Policy
- New Hire Information Security Awareness Training & Policy Awareness

Applicable Standards/Regulations/Citations/References

- ISO 27001:2013
- New York Department of Financial Services Cybersecurity Regulations
- Health Information Portability and Protection Act
- General Data Protection Regulation
- California Consumer Privacy Act

Revision History

Date	Version Number	Updated By	Description of Update
9/4/19	1.0	TJ Hart	Initial Policy
9/19/19	2.0	TJ Hart	Updated Formatting
2/12/20	3.0	TJ Hart	Annual Policy Update Cadence Removed Governance Reference Added Security Policy reference
4/28/20	4.0	TJ Hart	New Policy format Policy Number Change 24 to 22
10/19/20	5.0	TJ Hart	Added reference to continual improvement in Section 7 Removed duplicate Section 5 Removed duplicate Section 1.2

3/15/21	5.0	TJ Hart	Annual Review and Approval
3/15/22	5.0	David Christensen	Annual Review and Approval
3/15/23	5.0	David Christensen	Annual Review and Approval