POLICY			
Policy Name	ISO Remote Access Policy		
Policy Number	ISO-P017	**Version Number**	5.0
Supersedes Policy	N/A	**Effective Date**	9/4/2019
Last Reviewed Date	3/15/2023	**Last Revised Date**	3/15/2023
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 is in place to ensure the protection of the confidentiality, integrity, and availability of customer and PlanSource data.

Responsibilities

PlanSource Personnel – PlanSource Personnel 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 Security – 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.

Table of Contents (if applicable)

Definitions

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.

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 Systems – This is any computer system or application that processes, maintains or stores information used by PlanSource to manage their global enterprise.

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.

Payment Card Industry – PCI information is debit or credit card information, such as cardholder name, card numbers, point of sale details, or other information related to an individual's electronic purchasing history.

Personally Identifiable Information – 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.

Protected Financial Information – This is any financial information about a person or company, including payment history, receivables, financial reports, bank accounts, etc.

Protected Health Information – PHI is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This includes any part of a patient's medical record or payment history.

Restricted Information: Restricted information refers to privileged or proprietary information that only authorized people are allowed to access, as articulated in the Data Classification Policy.

Information designated as "restricted" is deemed to have a profound impact on the business if lost or misused, the result of which may cause severe damage to PlanSource's global enterprise. Restricted information includes Personally Identifiable Information (PII), Protected Health Information (PHI) and user possesses, which provides an automated rotating numeric configuration and a personal PIN (personal identification number), that only the user knows. When these two authentication factors are combined it allows the user to access a system or network where the two-factor authentication is allocated.

Untrusted Source – A computing device which is not under full control or the user and/or whose integrity or security posture cannot be determined.

Two Factor Authentication – Two-factor authentication provides explicit identification of users by means of the combination of two different components. These components may be something

Related Document(s)
• Information Security Policy
Applicable Standards/Regulations/Citations/References
• ISO 27001:2013

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 19 to 17
3/15/21	4.0	TJ Hart	Annual Review and Approval
3/15/22	4.0	David Christensen	Annual Review and Approval
3/15/23	5.0	David Gilbert	Revised Remote Access Approval Process
3/15/23	5.0	David Christensen	Annual Review and Approval