POLICY			
Policy Name	ISO Data Classification Policy		
Policy Number	ISO-P021	**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 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 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 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

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 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 data 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;
- Report unauthorized use, access, or disclosure of data to the applicable organization.

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

Non-Disclosure Agreement – An “NDA” is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to 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.

Security Risk Assessment – This is an assessment of the information being classified by the Information Owner, using risk assessment methodology such as PlanSource Risk Assessment Guideline, to determine the criticality to PlanSource.

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 23 to 21
10/19/20	5.0	TJ Hart	Removed previous section 2.5 Procedure
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