POLICY			
Policy Name	ISO Information Security Risk Management Policy		
Policy Number	ISO-P012	**Version Number**	5.0
Supersedes Policy	N/A	**Effective Date**	9/4/2019
Last Reviewed Date	3/15/2023	**Last Revised Date**	4/28/2020
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 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

Control - A defined process or procedure to reduce risk.

Data - Information collected, stored, transferred or reported for any purpose, whether in computers or in hard copy.

Inherent Risk - Level of risk before Risk Treatments (controls) are applied.

Residual Risk - Level of risk that remains after Risk Treatments (controls) are applied to a given Risk.

Risk - The possibility of suffering harm or loss or the potential for realizing unwanted negative consequences of an event.

Risk Assessment - The process of taking identified risks and analyzing their potential severity of impact and likelihood of occurrence.

Risk Management - The ongoing management process of assessing risks and implementing plans to address them.

Risk Register - The central repository that is used to capture and document all identified Risks.

Risk Treatment - The process of managing assessed or identified Risks. Risk treatment options are risk avoidance (withdraw from), transference (sharing), reduction (modify or mitigate) and acceptance (retention).

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 14 to 12
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	Added ISSC for risk acceptance approval Annual Review and Approval