

POLICY			
<b>Policy Name</b>	ISO Asset Management Policy		
<b>Policy Number</b>	ISO-P003	<b>Version Number</b>	5.0
<b>Supersedes Policy</b>	N/A	<b>Effective Date</b>	9/4/2019
<b>Last Reviewed Date</b>	3/15/2022	<b>Last Revised Date</b>	3/15/2023
<b>Policy Owner</b>		<b>Approved By</b>	
<b>Name</b>	David Christensen	<b>Name</b>	Srinivasan Venkatramani
<b>Title</b>	CISO	<b>Title</b>	CTPO
<b>Date Approved</b>	3/15/2023	<b>Date Approved</b>	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.

*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.

## Table of Contents (if applicable)

1	Asset Inventory.....	Error! Bookmark not defined.
2	Ownership of Assets .....	Error! Bookmark not defined.
3	Acceptable Use of Assets .....	Error! Bookmark not defined.
4	Asset Classification .....	Error! Bookmark not defined.
5	Asset Labeling and Handling .....	Error! Bookmark not defined.
6	Media Management .....	Error! Bookmark not defined.
7	Return of Assets.....	Error! Bookmark not defined.

## Definitions

**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.

**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, gaining unauthorized access to sensitive information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging keystrokes.

**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.

## 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

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	Asset Inventory requirements updated
3/15/23	5.0	David Christensen	Annual Review and Approval