

POLICY			
Policy Name	ISO Compliance Policy		
Policy Number	ISO-P006	Version Number	5.0
Supersedes Policy	N/A	Effective Date	9/4/19
Last Reviewed Date	3/15/23	Last Revised Date	3/15/23
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)

1	Legislation and Contractual Requirements	Error! Bookmark not defined.
2	Intellectual Property Rights	Error! Bookmark not defined.
3	Protection of Records.....	Error! Bookmark not defined.

Definitions

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.

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 Facilities – 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, Information Users, or business partners working on behalf 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
4/14/20	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	Added sections around Compliance engagement and software management
3/15/23	5.0	David Christensen	Annual Review and Approval