POLICY			
Policy Name	ISO Backup Policy		
Policy Number	ISO-P004	**Version Number**	5.0
Supersedes Policy	N/A	**Effective Date**	9/4/19
Last Reviewed Date	3/15/22	**Last Revised Date**	4/13/20
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 PlanSource's Information Security policies, and reporting any suspicious system activity to management and Information Security.

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 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.

Tale of Contents (if applicable)

Definitions

Device – Any computing system (e.g. workstation, smart phones, notebooks, laptops, tablets, hard drive, etc.) capable of accessing, storing, and/or processing PlanSource Information Assets or networks.

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.

PlanSource Personnel – employees, partners, consultants, agents, vendors, distributors and contractors who use or are granted access to PlanSource facilities or information systems.

Mobile Device – Any hand-held computing or communication device such as a smart phone, wearable computing device, and tablet or notebook that runs a mobile Operating System, including but not limited to iOS™ or Android™, and is capable of accessing a computer network without being physically tethered to the environment. All laptops, and tablets or notebooks that run the Windows™ operating system are not considered a Mobile Device for the purposes of this policy and are specifically excluded from the scope of this definition.

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
4/13/20	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	Identified frequency for backups and testing requirements
3/15/23	5.0	David Christensen	Annual Review and Approval