POLICY			
Policy Name	ISO Physical & Environmental Security Policy		
Policy Number	ISO-P019	**Version Number**	5.0
Supersedes Policy	N/A	**Effective Date**	9/4/2019
Last Reviewed Date	3/15/2023	**Last Revised Date**	3/15/2023
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 Owner – This is an individual, organization, or entity that determines the value and classification of the information and associated system(s) assigned to them and provides appropriate disclosure, distribution, and protection requirements. The Information Owner has primary responsibility for the information assigned to them whether it is in their custody or in the custody of others. As such, the Information Owner must:

- Authorize the use of the information that is consistent with its intended purpose;
- Protect aggregate information adequately. At minimum, assign the highest classification of any data component and consider if the collective data requires a higher classification;
- Protect information from unauthorized use, access, disclosure, alteration, or disposal;
- Report unauthorized use, access, or disclosure of information to 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.

PlanSource Security-issued access badge - The badge issued by the Security Department for accessing the PlanSource buildings with the employee's name, PlanSource ID number, and image.

Physical Security - Access Control Operator (Regional Badge Rooms)

- to take the image of the individual, if possible,
- to receive and evaluate the image for the PlanSource Security-issued Access Control Badge, and
- to print and distribute the new badge.

Tale of Contents (if applicable)

Definitions

Badge Security - Badge Access is the electronic ability to enter a building or security area by using the PlanSource Security-approved Access Badge.

Contingent Worker - A contingent worker is an individual who is not a PlanSource employee but is providing a service to PlanSource. There are four (4) classifications:

- Contractor (Contractor access will not exceed 1 year),
- Consultant (Consultant access will not exceed 1 year),
- Vendor (Vendor access will not exceed 1 year),
- Partner (Partner access will not exceed 1 year).

Default Badge Access - every badge of each of the worker types would receive a specific group of perimeter accesses into PlanSource buildings.

PlanSource Host - a PlanSource employee who sponsors a non-PlanSource employee for a PlanSource badge.

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.

Restricted Information – Restricted information refers to privileged or proprietary information that only authorized people are allowed to access, as articulated in the Data Classification Policy.

Information designated as "restricted" is deemed to have a profound impact on the business if lost or misused, the result of which may cause severe damage to PlanSource's global enterprise. Restricted information includes Personally Identifiable Information (PII), Protected Health Information (PHI) and customer sourced information.

Secure Area – A location which limits access to users who are authorized by way of a device that prevents access to the items which need to be secured from unauthorized persons. These devices include but not limited to card access, key access, combination code access, biometric access or other approved devices which prevent access.

Security group - a group of security areas/buildings which are programmed as one area, i.e., campuses.

Related Document(s)

- Information Security Policy
- Systems Access Policy
- Remote Access 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 21 to 19
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	Revised access approval process and permanent badge process

3/15/23	5.0	David Christensen	Annual Review and Approval