POLICY			
Policy Name	ISO Cyber Security Incident Management		
Policy Number	ISO-P010	**Version Number**	5.0
Supersedes Policy	N/A	**Effective Date**	9/4/2019
Last Reviewed Date	3/15/2023	**Last Revised Date**	10/15/2020
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

Security Incident Response Team – The SIRT is responsible for managing the successful resolution of security incidents or security breaches reported by PlanSource Personnel. The SIRT has full authority to take whatever action is deemed necessary to resolve an incident or breach in order to return the PlanSource business to normal productivity as quickly as possible.

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 and potential weaknesses 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

Security Incident Response Team – The SIRT is comprised of PlanSource Personnel trained in managing security incidents that occur which have an impact on PlanSource's business continuity. This team will identify the severity of the incident and perform the activities needed to resolve the situation and make recommendations to eliminate a future reoccurrence of the incident.

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 Cyber Security Event – An identified occurrence of a system, service or network state indicating a possible breach of information security or failure of safeguards, or a previously unknown situation that may threaten the security of PlanSource data.

Information Cyber Security Incident – A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening the security of data within PlanSource to include incidents like DDOS attacks.

Information Systems – This is any computer system or application that processes, maintains or stores information used by PlanSource to manage their global enterprise.

Personally Identifiable Information – PII is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. PII can be any information about an individual including information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.

Protected Health Information – PHI is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This includes any part of a patient's medical record or payment history.

Restricted Information – This classification applies to the most sensitive business information that requires the highest level of scrutiny to ensure limited access to only authorized PlanSource Personnel. Information designated as "restricted" (e.g. Personally Identifiable Information, Protected Health Information, and customer sourced information)

is deemed to have a profound impact on the business if lost or misused, the result of which could seriously and adversely impact PlanSource, its shareholders, employees, customers and business partners.

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
10/16/2020	5.0	TJ Hart	Update definitions: Security Event and Security Incident Added: … potential weaknesses to PlanSource Personnel Def. Added **Severity P5** (“Very Low”) - An event that is very informational and provides mainly insight into opportunities for threat intelligence and configuration optimization. Added Lessons Learned section.
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	Annual Review and Approval