Information Security Policy

Purpose

Campbell Page's Information Security Policy underscores our commitment to stringent compliance and the safeguarding of information, integral to our IT and cyber security strategy. It establishes a robust framework for protecting both proprietary and client information, ensuring regulatory compliance, and nurturing trust within the community for which we serve.

Scope

The policy encompasses all individuals interacting with our information systems, including employees, contractors, and third-party users. It covers the management and use of Campbell Page's vast array of information system resources, and information in various formats. The focus is on maintaining the confidentiality, integrity, and availability of our information and systems.

Objective

Our primary goal is to safeguard the confidentiality, integrity, and availability of information, crucial for client service and regulatory compliance. The policy emphasises operational continuity, threat minimisation, and impact reduction of security incidents. It also ensures adherence to legal, regulatory, and compliance requirements, incorporating information security principles into Campbell Page's operational and strategic planning.

Roles and responsibilities

Head of IT and also Acting CISO: Holds the primary responsibility for leading Campbell Page's information security and strategy. This includes overseeing system strategy, aligning with ISO27001/RFFR standards, ensuring compliance with policies and regulations, managing system security risks, and leading cyber security incident response. The Head of IT also plays a vital role in strategic planning, advising senior management, and steering committee participation.

All employees and stakeholders: All members of Campbell Page, including employees and external stakeholders, are responsible for adhering to the information security policies, and reporting security incidents, including obligations required of them when interacting with the Campbell Page system.

Implementation of policy

Campbell Page adopts a proactive approach to information security, aligning with ISO27001 standards and employing risk management to assess and control risks. This approach, emphasising legal and statutory compliance, ensures the security and integrity of our information systems, reflecting our commitment to robust information security practices.

Information Security Policy v.1.0 effective date: May 2024.