CAYLENT

THIRD PARTY VENDOR MANAGEMENT POLICY

Purpose and Goals

This Third-Party Vendor Management Policy, governed by the IT Department and the Legal Team, is an initiative to reduce the risk to Caylent resources from Third-Party Providers. The purpose of this Policy is to ensure that all vendors have appropriate controls to minimize risks that could adversely impact Confidentiality, Availability, and/or Integrity of their respective services or products.

Scope

This Policy applies to all Caylent operations and Caylent employees, as well as Third-Party Providers including: contractors, consultants, temporary employees, and other authorized entities performing duties on behalf of Caylent.

Definitions

The terms defined below apply throughout this Policy:

"Availability" means ensuring timely and reliable access to Information based upon the concept of Least Privilege, for authorized use.

"Confidentiality" means preserving authorized restrictions on Information access and disclosure, including means for protecting personal privacy and proprietary information.

"Contractor" means a person or a company that undertakes a contract to provide materials or labor to perform a service.

"Data" means an element of information in the form of facts, such as numbers, words, names, or descriptions of things from which "understandable information" can be derived.

"Information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

"Information Technology Resource(s)" means any equipment or interconnected system or subsystem of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by Caylent directly or by a third party under a contract with Caylent, which requires the use of such equipment. The term includes, but is not limited to: computers, mobile devices, software, firmware, services (including support services), and Caylent's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

"Information System" means inter-related components of Information Technology Resources working together for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

"Integrity" means ensuring records and the Information contained therein are accurate and authentic by guarding against improper modification or destruction.

"Third-Party Provider" means an authorized external entity, including, but not limited to, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums and investors, with or without a contractual relationship to Caylent.

Third Party Management

1. Initial Screening

- All Caylent departments engaging third-party IT products or services are required to undergo a security risk review of the requested product or service.

- Based on the security review performed, the Caylent IT Department will determine if a comprehensive security assessment will be required prior to entering into any agreement with the vendor.

2. Comprehensive Security Assessment

- The Third-Party Provider must complete a security questionnaire, and/or provide a copy of their most recent independent security audit or certification reports (i.e., SOC 2, ISO 2700x certification).

- The IT Department will review the security assessment and determine whether the Third-Party Provider complies with

Caylent's security requirements. If the Third-Party Provider is non-compliant, compensating controls will need to be assessed and implemented.

Contracting Agreements

Third-Party Providers that will store, process or transmit Data must:

- Sign a Data Processing Agreement (DPA) if applicable.
- Permit inclusion of Caylent standard security clauses and language in all relevant contracts, which addresses:

1. Compliance with Caylent security policies, right to audit, right to access, right to monitor, and compliance with applicable regulations where applicable.

2. A commitment from the Third Party Provider that the Third Party Provider agrees not to engage in improper business conduct, such as bribery, with the intent to improperly influence behaviors or obtain any benefit for Caylent.

3. A detailed description of the scope of the services to be provided by Third-Party Provider.

4. A clear description of how Caylent will compensate the Third-Party Provider for its services.

5. A formal acknowledgment by the Third-Party Provider that the Third-Party Provider understands the requirements of local anti-bribery laws and that the Third-Party Provider agrees not to violate them.

6. An agreement by the Third-Party Provider to certify, on a periodic basis, that it has not violated any anti-bribery laws while conducting Caylent business.

7. An agreement that the Third-Party Provider will not subcontract its services without Caylent's written permission.

8. Permission for Cayent to audit the Third-Party Provider expenses and invoices.

9. A requirement that the Third-Party Provider will inform Caylent if it is making payments of any kind to foreign officials.

Subsequent Reviews

Security reviews for third-party providers will cover a single use case and are required upon a new solution acquisition, changes in scope or use cases for current solutions, changes in system design or controls, business transfer, merger, or acquisition, and upon the renewal of current solutions.

Periodic review of a Third-Party Provider's security posture and continued compliance will be conducted as needed, based upon changes in system use, design or controls, contract renewal or business transfer, merger, or acquisition.

Exceptions

Exceptions to this Policy should be submitted to the General Counsel for review and approval. If an exception is requested, a compensating control or safeguard should be documented and approved.

Revision History

Original publication: March 28, 2022
Reviewed & Revised: February 2024