



VERSION 1.0

FOR INTERNAL PURPOSE ONLY

THIRD-PARTY DUE-DILIGENCE POLICY

Document Control Section

Document Control:

Author

<u>Draft</u>	<u>Author</u>	<u>Date</u>
1.0	Compliance Team	09/12/2022

<u>Classification</u>	<u>Storage Location</u>
Confidential	Shared folder

Owner

<u>Owner</u>	<u>Version</u>	<u>Date</u>	<u>Reviewed Draft Version</u>
Vikram Singh	1.0	09/12/2022	1.0

Reviewer

<u>Reviewer</u>	<u>Version</u>	<u>Date</u>	<u>Reviewed Draft Version</u>
Chandra Sekhar Garimel	1.0	09/12/2022	1.0

Approval

<u>Approver</u>	<u>Version</u>	<u>Date</u>	<u>Reviewed Draft Version</u>
Esha Chakravarty	1.0	09/12/2022	1.0

Release

<u>Release Version</u>	<u>Date Released</u>
1.0	09/12/2022

Change Control

<u>Version</u>	<u>Change Reason</u>	<u>Effective Date</u>
1.0	Nil	09/12/2022

Statement of Confidentiality

This document contains proprietary confidential information to be used solely for evaluating CtrlS Services Private Ltd, its group companies and affiliates. The information contained herein is to be considered confidential. All parties, by receiving this document, agrees that neither this document nor the information disclosed herein, nor any part thereof, shall be reproduced or transferred to other documents, or used or disclosed to others for any purpose except as specifically authorized in writing by CtrlS Services Private Ltd.

Contents

1 PURPOSE 5

2 GOVERNANCE 5

3 SCOPE 5

4 DEFINITIONS 5

5 DUE DILIGENCE APPROACH 7

6 ONGOING MONITORING 9

7 ANTI-MONEY LAUNDERING CHECK 10

8 PAYMENTS/RECEIPTS 10

9 TERMINATION OF THIRD PARTY 10

10 EXCEPTIONAL CASES 11

11 TRAINING PROGRAM 12

12 ANNEXURE 13

ANNEXURE A 13

ANNEXURE B & C 14

1 PURPOSE

This Policy outlines the requirements and processes that must be followed for CtrlS, its group companies, subsidiaries, and affiliates to work with third-party business partners. It sets out due diligence procedures for carrying out business with third parties to ensure commitments to establishing long-term relationships that are set on a strong foundation and to protect the business from risk arising from suppliers, customers.

The purpose of this policy is to enable CtrlS to make informed decisions about who they associate with to avoid potential problems affecting its business ethics, values, compliance, regulations, and public reputation. The guidelines in this Policy should be read in conjunction with:

- a) The Anti-Bribery and Anti-Corruption Policy
- b) Any other relevant policies as may be implemented from time to time

2 GOVERNANCE

- 2.1 Post adoption of the policy by the Board, any changes to this policy shall be tracked and documented for future reference and all changes shall be performed only after prior approval of the Compliance Committee headed by Chief Compliance Officer.
- 2.2 Compliance Committee headed by Chief Compliance Officer shall monitor the effectiveness and review the implementation of the compliance principles outlined in this policy, regularly considering its suitability, adequacy, and effectiveness.
- 2.3 Compliance Committee headed by Chief Compliance Officer shall be approached for any guidance regarding the Policy.

3 SCOPE

This policy applies to CtrlS, its group companies and affiliates (each entity shall be referred to as “Company” for this document) its Customers, Subcontractors, Service Provider, Suppliers, and Vendors.

All the persons who may be involved in any process or activity related to the third parties, for the services provided to or by CtrlS shall mandatory follow this Third-Party due diligence policy in case of both new and existing third parties.

4 DEFINITIONS

The following definitions are provided to assist you in understanding the policy:

- 4.1 **Due Diligence:** Due diligence is a process of investigation, into the details of a potential decision making such as an examination of operations, management, and the verification of material facts relating to the third parties. It entails conducting inquiries for timely, sufficient, and accurate disclosure of all material statements/information or documents, which may influence the outcome of the process.
- 4.2 **Third Party:** Third Party/Parties” means a party or parties with whom CtrlS, its group companies and affiliates do business or seek to do business, whether as a Customers, Subcontractors, Service Provider Suppliers, and Vendors, or otherwise, but for purposes hereof shall specifically exclude government agencies.

Defining Third Parties

- Contractor and sub-contractor: A contractor is a non-controlled individual or organization that provides goods or services to an organization under a contract. A subcontractor is an individual or organization that is hired by a contractor to perform a specific task as part of the overall project.
- Supplier/vendor: An individual or organization that supplies parts or services to another organization.
- Service provider: An individual or organization that provides direct/support services to CtrlS or its customers (e.g., communications, processing services).
- Customer: The recipient of the services offered by CtrlS or any of its affiliates/group companies.

4.3 Beneficial owner: This means an individual who ultimately owns or controls a client of CtrlS or the person on whose behalf a transaction is being conducted and includes a person who exercises ultimate effective control over a judicial person.

4.4 Key Managerial Personnel: Key managerial persons include the following persons who are vested with the principal roles to ensure the well-ordered functioning of the business:

- Chief executive officer, Managing Director.
- Company Secretary.
- Whole-time Director.
- Chief Financial Officer.
- Such other officers are designated by the Board as KMP but are not more than one level below the directors in whole-time employment.

4.5 Anti-Money Laundering: Anti-money laundering (AML) refers to the web of laws, regulations, and procedures aimed at uncovering efforts to disguise illicit funds as legitimate income.

4.6 Politically exposed person (PEP): A PEP is an individual who holds a prominent public position or role in a government body or international organization, either in India or overseas. Immediate family members and/or close associates of these individuals are also considered PEPs. PEPs often have power over government spending and budgets, procurement processes, development approvals, and grants. Examples of PEPs include heads of state, government ministers or equivalent politicians, senior government executives, high-ranking judges, and high-ranking military officers.

4.7 Emergency Services: Any services to be rendered on an urgent basis, with limited or no time to perform the third-party due diligence (background check).

4.8 Risk Management Team: CtrlS's Risk Management Team consist of the following members:

1. Mr. Chanakya Levaka, Chairperson
2. Mr. Satyanarayana RNV
3. Mr. Royce Thomas
4. Mr. Vikram Singh
5. Mr. Chandra Sekhar Garimel

4.9 Compliance Committee: CtrlS's Compliance Committee consist of the following members:

1. Ms. Esha Chakravarty, Chairperson
2. Mr. Venkata Niranjana
3. Mrs. Prachitha Kuchkulla
4. Mr. Satyanarayana RNV

5 DUE DILIGENCE APPROACH

5.1 Roles and responsibilities

Any CtrlS employee who on-boards / appoints any third party for services shall be responsible for performing the third-party evaluation, and a member of the Risk Management team is required to conduct the due diligence of such third party being appointed. Due diligence procedure shall be performed using the procedure as laid down in this policy.

The Risk Management team may outsource the due diligence function to any third party on behalf of CtrlS.

5.2 Obtaining and analyzing Know Your Client (KYC) information:

As a process of third-party onboarding, the Risk Management Team shall obtain sufficient Know Your Client (KYC) information of the third party to confirm the identity and be able to assess the reputational and financial risks to CtrlS. CtrlS shall identify what KYC information is required, considering CtrlS’s minimum requirements [\(Refer to Annexure A\)](#) and obtaining any additional information required by local legal and regulatory requirements. CtrlS shall specify the criteria for different levels of KYC information required and communicate this to the customer/vendor.

Where any personnel have personal or local business knowledge of a third party or its management or owners, this shall be considered, but this shall only supplement and not replace the KYC information gathering required under this procedure.

5.3 Risk assessment:

The third-party risk assessment shall be carried out for existing and proposed third parties based upon the information obtained as part of KYC information gathering and his or her own knowledge, Risk Management Team shall be responsible for undertaking and documenting the assessment of the third party and for confirming the accuracy and completeness of the due diligence. The third-party risk assessment process includes:

- Screening of the entity and each owner through open-source database that includes:
 - Media information through search engines,
 - Litigation records through search engines,
 - Government database - MCA Database and OFAC (Office of Foreign Assets and Control) check,
 - Key word search through search engine [\(Refer Annexure B for detail process understanding\)](#)

5.4 Classification of the Third party:

a) Based on the above risk assessment procedure performed, the third party shall be classified as Low, Medium, or High risk applying reasonable analysis and judgment.

Risk classification	Due diligence results and criteria
Low	No potential risk or conflicts identified based on checks defined in Risk assessment - 5.3
Medium	a. Below three (number) legal cases (Civil) affecting the future of the organization. b. Few negative findings based on Key word search.

High	<ul style="list-style-type: none"> a. Identified risks based on PEP (politically exposed person). b. Identified findings against person of interest (Promoters/ KMP's/ Directors). c. High Risk of default based on debt< auditors report. d. Multiple legal cases (Civil / Criminal / others) affecting the future of the organization. e. Conflict of Interest based on MCA website. f. Multiple Negative findings based on Key word search. g. Companies in the Arms, Gambling, Government / Public sector. h. OFAC (Office of Foreign Assets and Control) check negative finding.
------	--

b) Third-party services that do not represent the requisite level of third-party risk, do not support the key functions and products and are easily replaceable, well-known public enterprises, individuals who have a reliable source of funds, and the person with whom small transactions are entered into / proposed to be entered can be classified as low-level risk.

5.5 Final Decision

Based on the results of the due diligence review, the feasibility of the proposed business transaction shall be assessed by the Risk Management team.

A third-party risk assessment report is prepared based on the evaluation performed by the risk assessment team. In case of Medium/ High risk appropriate mitigation actions are prepared ([Refer Annexure C](#)) against each finding by the concerned team and submitted for a review to the Risk Management team.

Based on mitigation actions and responses Risk Management team provides the approval as per the delegation of authority ([refer section 5.7](#)). No Third Party will be onboarded until all high risk have been resolved and mitigation actions and responses documented, and approvals obtained as per the DOA.

5.6 Approval Process

Once due diligence processes are complete, the management/concerned department head shall decide whether to move forward with the proposed new party or continue with the existing third party and shall forward the proposal made along the supporting documents to the concerned approving authority as mentioned below.

Both the department head and the approving authority shall critically review the evaluation and identify whether:

- a) Additional information is required, or any further evaluation needs to be conducted
- b) Identified risks have been mitigated or reduced to an acceptable low level by adopting appropriate risk mitigation strategies
- c) The third party can be onboarded or continued for limited services

Risk rating	Approval required
Low risk	Risk Management Committee
Medium	Risk Management Committee
High-risk	Risk Management Committee, Compliance Committee, and CRO jointly.

d) All documentation relating to the risk assessment and due diligence processes, and the evaluation of risk, should be signed by the parties responsible and retained by the organization.

5.7 Documentation

It shall be the responsibility of the Risk Management Team to adequately document all the information obtained, significant assumptions and judgments made during the process of conducting due diligence, and results of the due diligence in electronic form. The following document(s) shall be readily made available for reference as required.

- a) Background verification documents.
- b) Risk assessment form ([Refer Annexure C](#))
- c) Risk categorization of existing and new vendors.
- d) Disqualification of third party and deletion from the approved third-party list and contract termination.

6 ONGOING MONITORING

6.1 The Risk Management Team, shall perform ongoing monitoring of the transactions which involves identifying changes in the third-party profile, business dealings, products and services offered, associations, partnerships, or any business restructuring through recurring Internet and database searches, review of the third party's payment requests, etc.

6.2 This process shall be carried out to uncover any changes in the expected patterns which are indicative of suspicious transactions, non-compliances, money laundering or deception, etc., and to determine whether information obtained is consistent with the Could4C's information about that third party, nature, and purpose of the business relationship.

6.3 To adequately monitor and mitigate the risk, CtrlS shall consider implementing the following:

- a) Retain a contractual right of termination in case, the information provided to us is found to be incorrect/misleading/false.
- b) Conduct / cause to conduct audit of the third party.
- c) The individual team member of respective business units/ functions shall update the Vendor Master, Customer Master, and other master data relating to the third parties for the changes in the risk profile if any.
- d) Any identified violations of the Anti-bribery policy of CtrlS shall be duly communicated to the concerned department. (***Refer to Section 1, Clause 3 – Reporting of Violations of CtrlS 's ABAC Policy.***)
- e) Where appropriate, disqualify/terminate the third-party ([Refer to Clause 9 for disqualification/termination](#))
- f) The Due diligence records shall be updated for any changes or additional information obtained during the ongoing monitoring process.

6.4 Frequency of due diligence:

- a) The due diligence process is required to be repeated at regular intervals including, but not limited to:
- b) Contracts/ agreements renewals.
- c) Failure by a third party to meet the contract requirements.
- d) A significant amendment to the contract (e.g., Nature of transaction/scope of services, etc.)
- e) Anticipated/ actual changes in the KMP/Promoters or Board of the third party.
- f) Due diligence based on time:
 - Low – Once every 3 years.
 - Medium – Once every 2 years.
 - High – Annually.

7 ANTI-MONEY LAUNDERING CHECK:

CtrlS shall conduct business only with reputable third parties who are involved in legitimate business activities and whose funds are derived from legitimate sources. Risk Management team during onboarding and ongoing monitoring also reviews:

- a) Changing banks, several times in a short space of time.
- b) Attempts to disguise the real owner of the business.
- c) Requests for facilitation or speed in transactions.
- d) A large amount of private funding from an individual running a cash-intensive business.
- e) False or suspicious documents used.
- f) A large number of cash transactions inconsistent with the profile of the customer.
- g) Business transactions involve countries with a high risk of money laundering and/or funding terrorism.

8 PAYMENTS/RECEIPTS

CtrlS employees should take particular care with regard to the following circumstances which may incite suspicion or can be regarded as possible ways of money laundering or red flags:

- a) Payments where the ultimate beneficiary is not identified.
- b) Payments that are not specified in the corresponding contract or are made to third parties or bank accounts unrelated to the transaction.
- c) Complex deal structures or payment patterns that reflect no real business purpose or economic sense.
- d) The purchase of products, or a larger volume purchase, that appears to be inconsistent with a customer's normal ordering pattern, and in the absence of any legitimate business reason such as a special price promotion.
- e) Requests to receive payments urgently or ahead of schedule.
- f) Unusual or unconventional arrangements for the transfers of funds coming from or going to countries with strict banking secrecy laws, weak anti-Money Laundering controls, tax havens, or where corruption is known to be widespread.
- g) Cash payments/collections and transfers that are not consistent with the counterparty's normal business activities.
- h) Transactions involving unusual or unconventional payment or settlement methods or parties or places unrelated to the transaction.

Any identified/ suspected instances as mentioned above shall be reported to the Compliance Committee headed by Chief Compliance Officer at CCO@ctrls.in and the process of due diligence shall be conducted to determine the effect on CtrlS's business and reputation.

9 TERMINATION OF THIRD PARTY

A third-party relationship may be terminated on the basis of the information obtained subsequent to acceptance of the business relationship with the third party, which might result in operational, financial, reputational risks or other reasons. The following indicators may be considered while deciding on terminating the third party:

- a) Non-compliance with CtrlS's policies and procedures including ethical business standards.
- b) Failure to comply with the contractual/agreed terms.
- c) Company/ person declared as insolvent by a competent court until the period of insolvency is not resolved.
- d) Resorting to malpractices / illegal activities that resulted in or might result in financial/ reputational damage to CtrlS.

- e) Using CtrlS's assets/ rights/ names etc. to the third party's advantage.
- f) The business unit/function head must obtain approval from the CFO & CRO jointly to blacklist the third party along with the reasons.
- g) A blacklisted third party may be registered again only after obtaining prior approval from CFO & CRO jointly and documenting the reasons for the same.

10 EXCEPTIONAL CASES

- 10.1 In certain exceptional circumstances, such as emergency services, close timelines, etc., a third party can be onboarded without performing the due diligence procedure as laid down.
- 10.2 However, the department head shall ensure that the due diligence process is carried out later, not more than 30 days after onboarding, and adequate approval from the CFO & CRO jointly shall be obtained.
- 10.2 CtrlS shall ensure that the minimum documentation/information as specifies in the below table has been obtained:

For Vendors:

Transaction Limits	Documents Required
Below 1 million INR	KYC: GST Certificate, PAN, Aadhar, Bank Details on letter head, MSME if applicable
Above 1 million INR	<ul style="list-style-type: none"> • KYC: Document GST Certificate, PAN, Aadhar, Bank Details on letter head, MSME if applicable • TAN, Proof of registered office, Registration certificate, License, and Contact • Credit Rating / Credit Scores • Financial Statements • Copy of ITRs for 2 consecutive years • Organization and ownership details • Details of any beneficial owners of the Company <p><i>For detail refer Annexure A</i></p>

For Customers

Transaction Limits	Documents Required
Below 5 million INR	KYC: PAN, Aadhar
Above 5 million INR	<ul style="list-style-type: none"> • KYC: Document GST Certificate, PAN, TAN, Registration certificate, License, and Contact • Credit Rating / Credit Scores • Financial Statements • Copy of ITRs for 2 consecutive years • Organization and ownership details • Details of any beneficial owners of the Company • KMP's <p><i>For detail refer Annexure A</i></p>

11 TRAINING PROGRAM

CtrlS shall conduct training programs so that the members / concerned staff are adequately trained and kept informed about the due diligence procedures.

Mandatory training shall be provided annually and as and when changes are made in the policy or any new procedures are implemented in the process of due diligence.



12 ANNEXURE

ANNEXURE A

List of Preliminary Checks for Onboarding
Customer & Vendor

- KYC Details: Document GST Certificate, PAN, Aadhar, Bank Details on letter head, MSME if applicable
- Credit Rating / Credit Scores
- Financial Statements
- Copy of ITRs for 2 consecutive years
- Organization and ownership details (Example: List of officers and directors, list of shareholders, Org. chart, etc.)
- Basic information about the CEO, other executives/KMPs, and Board members
- An overview of the Company's corporate structure
- Certain business information such as Registered corporate Name, Registration number, License
- Details of any beneficial owners of the Company. (These are the individuals who directly or indirectly own more than 25% of the Company or otherwise exercise significant control over it. After the beneficial owners are identified, they must be verified.
- Obtain a signed statement that no conflict of interest exists from the third parties, and it has not been prosecuted /investigated for any offence involving moral turpitude or otherwise which is punishable under any law whether in/outside India

ANNEXURE B & C

Keyword Search Process (Annexure A)	 Keyword Search Process
Risk Assessment Form (Annexure B)	 Risk Assessment Form