03 January 2022

SEGREGATION OF DUTIES GUIDELINES

Compliance Team

CTRLS DATACENTERS LTD
CLOUD4C SERVICES PVT LTD

DOCUMENT CONTROL:

PREPARATION

Draft	Author	Date
1.0	M.Venkataniranjan	30-03-2017
1.1	M.Venkataniranjan	06-01-2018
1.2	M.Venkataniranjan	10-10-2018
1.2	M.Venkataniranjan	05-01-2019
1.2	M.Venkataniranjan	02-01-2020
1.2	Vasanth Garimella	30-12-2020
1.2	Vamsi Krishna Muvva	31-12-2021

REVIEW & APPROVAL

Reviewer and Approver	Version	Date	Reviewed Draft Version
R.S.Prasad Rao	1.0	16-04-2017	1.0
R.S.Prasad Rao	1.1	07-01-2018	1.1
R.S.Prasad Rao	1.2	10-10-2018	1.2
RS Prasad rao	1.2	07-01-2019	1.2
RS Prasad rao	1.2	03-01-2020	1.2
RS Prasad rao	1.2	01-01-2021	1.2
RS Prasad rao	1.2	03-01-2022	1.2

RELEASE

Release Version	Date Released
1.0	16-04-2017
1.1	07-01-2018
1.2	10-10-2018
1.2	07-01-2019
1.2	03-01-2020
1.2	01-01-2021
1.2	03-01-2022

DISTRIBUTION LIST

Name	Designation	Department
NOC Teams	SM Managers	
COE Teams	COE Leads	

CHANGE CONTROL

Version	Change Reason	Effective Date
1.1	Reviewed with no updates	07-01-2018

1.2	Reviewed and added Training section - 7, Review of the policy section - 8	10-10-2018
1.2	Reviewed and no updates	05-01-2019
1.2	Reviewed and no updates	03-01-2020
1.2	Reviewed and no updates	30-12-2020
1.2	Reviewed and no updates	31-12-2021

STATEMENT OF CONFIDENTIALITY

This document contains proprietary trade secret and confidential information to be used solely for evaluating CtrlS Datacenters Ltd. The information contained herein is to be considered confidential. Customer, 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 Datacenters Ltd.

CONTENTS

1. PURPOSE

CtrlS grants its employees the privilege of using portable devices of their choosing at work for their convenience. CtrlS reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

2. INTRODUCTION

Segregation of Duties is the separation of incompatible duties that could allow one person to commit and conceal fraud that may result in financial loss or misstatement to the company. Segregation of duties may be within an application or within the infrastructure. It represents a key internal control that ensures no single person has too much influence over any business transaction or operation. It serves to prevent unintentional errors or fraud and ensure timely detection of errors that may occur. Further, it provides a method of improving organizational, business process and IT control alignment. Segregation of duties has always been an important component of a properly functioning internal control environment.

3. PURPOSE OF SEGREGATION OF DUTIES

Adequate segregation of duties reduces the likelihood that errors (intentional or unintentional) will remain undetected by providing for separate processing by different individuals at various stages of a transaction and for independent reviews of the work performed. The segregation of duties provides four primary benefits:

a) the risk of a deliberate fraud is mitigated as the collusion of two or more persons would be required in order to circumvent controls;
b) the risk of legitimate errors is mitigated as the likelihood of detection is increased;
c) the cost of corrective actions is mitigated as errors are generally detected relatively earlier in their lifecycle; and
d) the organization’s reputation for integrity and quality is enhanced through a system of checks and balances.

Segregation of duties is a basic, key internal control and one of the most difficult to accomplish. In essence, there is greater assurance that internal control responsibilities will be fully deployed when there is increased dispersion of such responsibilities among multiple individuals and work groups.

4. SCOPE

This policy is applicable to employees, contractors and third party vendors working at CtrlS Datacenters facility.

5. PRINCIPLE OF SEGREGATION OF DUTIES

The key principle of segregation of duties is that an individual or small group of individuals should not be in a position to control all aspects of a transaction or business process. Basically, the general duties to be segregated are: planning/initiation, authorization, custody of assets, and recording or reporting of transactions. In addition, control tasks such as review, audit, and reconcile should not be performed by the same individual responsible for recording or reporting the transaction.

The principle of segregation of duties generally helps define the constructs that will govern the definition of processes, controls and reporting structures of organizational units.

The principle of segregation of duties in an information system environment is also critical as it ensures the separation of different functions such as transaction entry, on-line approval of the transactions, master file initiation, master file maintenance, user access rights, and the review of transactions. In the context of application/server level controls, this means that one individual should not have access rights that permit them to enter, approve and review transactions. Therefore, assigning different security profiles to various individuals would support the principle of segregation of duties.

6. IDENTIFICATION OF SEGREGATION OF DUTIES ISSUES

a) Each functional business area shall be responsible for developing and implementing a schedule for assessing its area for potential or actual segregation of duties on a recurring basis.

b) Each functional business area shall formally evaluate its area for the existence of potential or actual segregation of duties issues on a periodic basis.

c) Organizational segregation of duties issues shall be considered during the periodic evaluations. The positioning of the business area in company, its relationships with other functional business areas, and the nature of its responsibilities shall be considered.

Functional segregation of duties issues shall be considered during the periodic evaluations. The assigned job functions of personnel in the business area shall be considered from a standpoint of incompatible duties.

e) Technological segregation of duties issues shall be considered during the periodic evaluations. The assigned system and application security of personnel shall be considered from a standpoint of access within systems to perform incompatible functions.

7. REMEDIATION OF SEGREGATION OF DUTIES ISSUES

a) Each functional business area shall document the segregation of duties issues identified during the formal periodic evaluations.
b) The nature of the issue and the involved parties/systems shall be included in the documentation of the segregation of duties issues.
c) Business area management shall review the documentation and determine remediation options for each issue.
d) Remediation options may include a combination of corrective or mitigating measures.
e) Business area management shall document the selected remediation method, along with the effective date of the remediation.

Senior management and Internal Audit shall be provided copies of all documentation relating to segregation of duties analysis and remediation.

8. TRAINING

CtrlS shall ensure all team members undergo periodical training outlined in this policy.

9. REVIEW OF THE POLICY

- This document will be reviewed and updated on an annual basis or when significant changes occur to the organization systems and information security standards.

10. VIOLATION WITH THE POLICY

Any user found to have violated this Policy may be subjected to disciplinary action, up to and including termination of employment.

11. CONSEQUENCES OF VIOLATION OF THE POLICY

Disciplinary action shall be consistent with the severity of the incident, as determined by an investigation, and may include:

- As deemed appropriate by Management, Human Resources, and the Legal Department.

Contact role for clarification regarding the Policy

The sponsor of this policy is the Head – Information Security. Head – Information Security – CtrlS shall be responsible for maintenance and accuracy of the policy. Any questions regarding this policy shall be directed to the Head – Information Security.

12. WAIVER CRITERIA

This Policy is intended to address information security requirements. Requested waivers shall be formally submitted to the Head – Information Security including justification and benefits attributed to the waiver for approval. The waiver shall only be used in exceptional situations for communicating non-compliance with the policy for a specific period of time (subject to a maximum period of 30 days). At the completion of the time period the need for the waiver shall be reassessed and re-approved, if necessary. Waiver shall not be provided for more than three consecutive terms. The waiver shall be monitored to help ensure its concurrence with the specified period of time and exception.