03 January 2022

EXCEPTION POLICY (RISK ACCEPTANCE)

Compliance Team

CTRLS DATA CENTERS LTD

DOCUMENT CONTROL:

PREPARATION

Draft	Author	Date
1.0	M.Venkataniranjan	08/01/2017
1.1	M.Venkataniranjan	06/01/2018
1.2	M.Venkataniranjan	10/10/2018
1.2	M.Venkataniranjan	05/01/2019
1.2	P Dali Naidu	02/01/2020
1.2	M.Venkataniranjan	30/12/2020
1.2	Vamsi Krishna Muvva	31/12/2021

Classification	Storage Location
Confidential	Shared folder

Review & Approval

Reviewer & Approver	Version	Date	Reviewed Draft Version
RS Prasad rao	1.0	16/01/2017	1.0
RS Prasad rao	1.1	07/01/2018	1.1
RS 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	16/01/2017
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

COE Teams	COE Engineers	Service Delivery
BU Heads		

Change Control

Version	Change Reason	Effective Date
1.1	Version updated	07/01/2018
1.2	Reviewed and Updated Training section - 8, Review of the policy section -9	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	31/12/2020
1.2	Reviewed and no updates	31/12/2021

STATEMENT OF CONFIDENTIALITY

CONTENTS

1. Introduction

Situations or scenarios will arise that cannot be effectively addressed within the constraints CtrlS security policies and standards. There will be times when business processes can and should take precedence over these policies. However, we must still consider the security of CtrlS infrastructure and data. The process allows BU unit heads and leadership to make an informed decision on whether or not to request an exception to a particular policy by understanding the risk and alternatives involved.

2. SCOPE

This policy shall be applicable to all employees of CtrlS, its contractors, subcontractors, associated third parties who are users of CtrlS services or who have access to CtrlS Information systems.

3. POLICY

- Any deviation from security policies and standards must be reviewed via the Information Security Exception Review process.
- The exception review process must involve respective Manager and Department Head.
- The exception review process must log all findings and results in a central repository that is accessible to all Georgia Tech staff involved in the assessment of the exception request.
- Approved exceptions must be periodically reviewed by respective Manager and the Business Unit Head requesting the exception.
- Exemption requests involving potentially significant risk to the Unit may require approval of the Business Unit Head.

4. EXCEPTION CRITERIA

- Exception requests must be evaluated in the context of potential risk to the Unit and CtrlS environment as a whole.
- Exception request evaluations must take into account what value the exception will bring to the Unit requesting the exception.
- Exception requests that create significant risks without compensating controls will not be approved in case it high risk.
- Exception requests must be consistently evaluated in accordance with CtrlS risk acceptance practice.

5. FLOW

- If a Business Unit (or Team) determines that they cannot follow Organisation policy or standard, or issue cannot be addressed as per Organisation policy or standard then the Business Unit (or Team) should request an exception. Before doing so, the Business Unit (or

Team) should consider what risks they may face by not adhering to the policy or not (issue is unresolved) as well as the benefit gained by requesting the exception.

- The Business Unit should fill out the Exception form (Risk Acceptance) and submit it to BU Head.
- BU Head will review the submission for completeness (ensure no information is missing).
- BU Head will perform a risk assessment of the request, the proposed mitigation, and the benefit of allowing the exception. The purpose of the review is to examine the exception request, and discuss the potential risk and proposed mitigation by the BU or Team. If the exception poses a significant risk, Respective BU or Team will work propose reasonable alternatives to both mitigate the risk as well as provide the necessary functionality needed by the Unit.
- If the review finds the exemption could lead to significant risk to the BU or Team or the organization, then they will inform the Business Unit Head.
- Once the review of the exception has been completed and the exception approved. In doing so, the Unit is accepting the potential risk caused by allowing the exception. An electronic copy of the exception will be maintained.
- The exception will be granted for a period of not more than 1 year from the time the exception is granted. At the end of the year, the exception will be reviewed and either terminated or renewed for another period
- This policy shall be published on the CtrlS QC website.

6. TRAINING

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

7. 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.