ASSET CLASSIFICATION POLICY

Document History

Ver. No	Authored by	Date Created	Description	Approved by	Approved Date
1.0	Sudheer G	10/04/2013	Base Document	R.S.Prasad Rao	16/04/2013

Revision History

Version#	Date	Author	Revision Description	Approved by	Approved Date
1.0	16/04/2013	Sudheer G	Baseline	R.S.Prasad Rao	16/04/2013
1.1	14/03/2014	Sudheer G	Added statement of Confidentiality, Reviewed and no update	R.S.Prasad Rao	14/03/2014
1.2	06/01/2015	Soudha Rahman	Reviewed and updated	R.S.Prasad Rao	31/03/2015
1.3	1/02/2016	Deepthi Naidu	Reviewed and no update	R.S.Prasad Rao	1/02/2016
1.5	8/06/2016	M.Venkataniranjan	Reviewed and Updated version	R.S.Prasad Rao	8/06/2016
1.6	8/01/2017	M.Venkataniranjan	Reviewed and Updated version and scope	R.S.Prasad Rao	16/01/2017
1.7	06/01/2018	M.Venkataniranjan	Reviewed and Updated version control	R.S.Prasad Rao	07/01/2018
1.7	31/12/2020	M.Venkataniranjan	Reviewed and Updated version control	R.S.Prasad Rao	01/01/2021

STATEMENT OF CONFIDENTIALITY

This document contains proprietary trade secret and confidential information to be used solely for evaluating Ctrl S 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 Ctrl S Datacenters Ltd.

TABLE OF CONTENTS

1. Introduction

All assets shall be accounted for and have a nominated owner. Assets including information assets shall be classified to indicate the need, priorities, and expected degree of protection when handling the assets. Assets have varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. Classifying assets allows information owners to control and restrict access to sensitive information in manner that is commensurate with the value of the information. Asset classification policy is defined to ensure CtrlS (Cloud4C) assets including all information assets are identified, properly classified, and protected throughout their lifecycles.

2. Objective

The objective of the Asset Classification policy is to define an appropriate set of protection levels and communicate the need for special handling measures.

3. Scope

This procedure shall be applicable to all employees of CtrlS (Cloud4C), its contractors, subcontractors, associated third parties who are users of CtrlS (Cloud4C) services or who have access to CtrlS (Cloud4C) facility. This policy collectively applies to all assets of CtrlS (Cloud4C) which shall include:

- Physical Assets,
- Service Assets,
- People Assets,
- Information Assets, and
- Software Assets.

Cloud4C Services Private Limited is Sister concern company of CtrlS Data centers Ltd. which is registered under the provisions of Companies Act,1956 having registered office at pioneer Towers, Plot No. L6, software Units Layout, Madhapur, Hyderabad, Telangana, 500081. The management and Support teams are same. Hence IT2SMS covers both CtrlS & Cloud4C.

4. Policy Statement

All CtrlS (Cloud4C) assets shall be classified and managed based on its confidentiality, sensitivity value and availability requirements. To ensure that confidentiality and sensitivity of information is maintained, an asset classification scheme has been designed for CtrlS (Cloud4C). The level of security to be accorded to the information of the company shall depend directly on the classification level of the asset which shall be associated with each asset.

4.1 Asset Classification Levels

Information owners shall identify all assets for the purpose of defining their value, criticality, sensitivity and legal implications based on the 3 criterions (Confidentiality, Integrity, and Availability).

4.1.1 Information Systems Asset Inventory

- CtrlS (Cloud4C) shall identify all its assets and list it in an Asset Inventory Sheet (*Refer: ISMS – Asset Register Template).*

- The Asset Inventory *(Refer ISMS – Asset Register)* shall contain the following information as a minimum:
    - Asset identification
    - Asset description
    - Asset location
    - Asset Owner/Custodian
    - Asset classification

4.1.1.1 Asset Classification Roles and Responsibilities

- Each asset shall have a designated Owner. The Owner shall be the person who either creates the information himself, or acts as an in-charge of the team producing the information.
- Each asset shall also have a nominated custodian (who may be separate from the Owner of the Asset).
- The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets.
- The asset owner / custodian shall be responsible for:
    - Ensuring that information and assets associated with information processing facilities are appropriately classified; and
    - Defining and periodically reviewing access restrictions and classifications, taking into account applicable access control policies.

4.1.1.2 Asset Classification Criteria

- All assets shall be classified according to this policy. All assets shall be handled according to the classification levels to ensure security of the information resource.
- Risk classification shall enable CtrlS (Cloud4C) to focus asset protection mechanisms on those assets that are most susceptible to specific risks. Assets shall be classified based on their susceptibility to risk.

4.1.1.3 Consistent Classification

- The assets shall be classified into the following categories:
    - **Public** – This classification shall apply to information that has been approved by CtrlS (Cloud4C) management for release to public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm.
    - **Restricted / Controlled** – This classification shall apply to less sensitive assets that are intended for use with in CtrlS (Cloud4C). Its unauthorized disclosure could cause little impact on CtrlS (Cloud4C), or its customers, suppliers, or business partners.
    - **Confidential** – This classification shall apply to sensitive assets that are intended for use within CtrlS (Cloud4C). Its unauthorized disclosure could adversely impact CtrlS (Cloud4C) or its customers, suppliers, business partners, or employees.
    - **High Risk** – This classification shall apply to the most sensitive assets that are intended for use strictly within CtrlS (Cloud4C). Its unauthorized disclosure could seriously and adversely impact CtrlS (Cloud4C), its customers, its business partners, stakeholders, and its suppliers.

The assets shall be labeled and secured appropriately based on the classification, from the time it is created until the time it is destroyed (*Refer: ISMS – Information Labeling and Handling Procedure and Media Handling Policy and Procedure)* or re-labeled. The labels shall be stuck on all media holding any information (hard copies, floppy disks, CD-ROMs, etc) and also on all other assets (Physical, Information, Services, People, and Software) *(Refer: ISMS – Asset Classification and Control Standard)*.

4.1.1.4 **Acceptable Use of Assets**

- CtrlS (Cloud4C) shall ensure that there shall be rules defined for the acceptable level of use *(Refer: ISMS – Acceptable Use Guideline)* for all the assets of the organization.
- CtrlS (Cloud4C) shall ensure that the employees, contractors and third parties follow the guidelines for the acceptable level of use of all the assets. Assets shall be used for business and operational purposes only and shall be protected from damage caused due to unauthorized usage.

5. Compliance with the Policy

Compliance with the Asset Classification Policy and Procedure shall be mandatory. Head Information Security–CtrlS (Cloud4C), assisted by information security forum shall ensure continuous compliance to this policy and procedure with in CtrlS (Cloud4C). Periodic review shall be conducted by Departmental Heads and shall be reported to Head – Information Security to verify compliance to this policy and procedure. All employees shall be responsible to inform the Head– Information Security, if any policy breach is discovered or identified.

6. Violation with the Policy

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

6.1 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, but not be limited to:

- Loss of access privileges to information assets, and
- Other actions as deemed appropriate by Management, Human Resources, and the Legal Department.

7 Contact role for clarification regarding the Policy

The sponsor of this policy is the Head Information Security – CtrlS (Cloud4C). Head Information Security – CtrlS (Cloud4C) shall be responsible for maintenance and accuracy of the policy. Any questions regarding this policy shall be directed to the Head Information Security – CtrlS (Cloud4C).

8 Waiver Criteria

This Policy and Procedure is intended to address information security requirements. Requested waivers shall be formally submitted to the Head Information Security – CtrlS (Cloud4C) 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.