CLOUD4C

01 January 2022

MEDIA HANDLING POLICY

Compliance Team

CLOUD4C SERVICES PVT LTD

DOCUMENT CONTROL:

Preparation

Draft	Author	Date
1.0	Sudheer G	16/04/2013
1.1	Sudheer G	14/03/2014
1.2	Soudha Rahman	1/6/2015
1.3	Deepthi Naidu	14/08/2015
1.4	Deepthi Naidu	1/02/2016
1.5	M.Venkataniranjan	8/06/2016
1.6	M.Venkataniranjan	8/01/2017
1.7	M.Venkataniranjan	06/01/2018
1.8	M.Venkataniranjan	10/10/2018
1.8	M.Venkataniranjan	05/01/2019
1.8	G Ajay	02/01/2020
1.8	Keerthana Ravikanti	31/12/2020
1.8	Swathi Bachanaboina	31/12/2021

Classification	Storage Location
Confidential	Shared folder

Review & Approval

Reviewer & Approver	Version	Date	Reviewed Draft Version
RS Prasad rao	1.0	17/04/2013	1.0
RS Prasad rao	1.1	14/03/2014	1.1
RS Prasad rao	1.2	1/6/2015	1.2
RS Prasad rao	1.3	14/08/2015	1.3
RS Prasad rao	1.4	2/01/2016	1.4
RS Prasad rao	1.5	8/06/2016	1.5
RS Prasad rao	1.6	16/01/2017	1.6
RS Prasad rao	1.7	06/01/2018	1.7
RS Prasad rao	1.8	10/10/2018	1.8
RS Prasad rao	1.8	07/01/2019	1.8
RS Prasad rao	1.8	03/01/2020	1.8

RS Prasad rao	1.8	01/01/2021	1.8
RS Prasad rao	1.8	01/01/2022	1.8

Release

Release Version	Date Released
1.0	17/04/2013
1.1	14/03/2014
1.2	1/6/2015
1.3	14/08/2015
1.4	2/01/2016
1.5	8/06/2016
1.6	16/01/2017
1.7	6/01/2018
1.8	10/10/2017
1.8	07/01/2019
1.8	03/01/2020
1.8	01/01/2021
1.8	01/01/2022

Distribution List

Name	Designation	Department
COE Teams	COE Engineers	Service Delivery
BU Heads		

Change Control

Version	Change Reason	Effective Date
1.0	Aligned to the CtrlS format, logo, added statement of Confidentiality & Reviewed	17/04/2013
1.1	Reviewed and no update	14/03/2014
1.2	Reviewed and no update	1/6/2015
1.3	Reviewed and no update	14/08/2015
1.4	Reviewed and updated version	2/01/2016
1.5	Reviewed and Updated version and scope	8/06/2016
1.6	Reviewed and Updated version control	16/01/2017
1.7	Reviewed with no update	6/01/2018

1.8	Reviewed and added Training section – 6, Review of the policy section -7	10/10/2017
1.8	No updates	05/01/2019
1.8	No Updates	03/01/2020
1.8	No updates	31/12/2020
1.8	No updates	31/12/2021

STATEMENT OF CONFIDENTIALITY

CONTENTS

1. INTRODUCTION

Information is created and stored in many formats on a variety of media. Media shall be anything on which information or data can be recorded or stored and shall include both paper and a variety of electronic media. Storage devices shall include but shall not be limited to: computer hard drives, portable hard drives, backup tapes, DVD/ CD W/RW, USB storage drives, blackberry, and other Personal Digital Assistants (PDA), cell phone, I pods, MP3 players, digital cameras, fax machines, photo copiers, and other types of portable storage devices like microchips.

Media can be used both to store sensitive information and to carry it from one location to another. To protect the information, one must safeguard the media against disclosure, theft, or damage. Proper media labelling, storage, transport, and disposal are risk mitigation controls. Consideration shall also be given to the nature of the information involved (how sensitive is the data), and the format in which it is held or stored. *(Refer: Asset classification Policy and Procedure).*

2. OBJECTIVE

This policy is intended to:

1.2 To ensure appropriate operating procedures are established to protect documents, computer media (e.g. tapes, disks) from unauthorized disclosure, modification, removal, and destruction.
1.3 All media irrespective of PII go through the secure disposal or re-use, equipment
1.4 To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.
1.5 To ensure media are controlled and physically protected.

3. SCOPE

This procedure shall be applicable to all employees of Cloud4C, its contractors, subcontractors, associated third parties who are users of Cloud4C services or who have access to Cloud4C Information systems.

4. POLICY STATEMENT

This policy relates to the use of Cloud4C media both electronic and print. The policy details the handling of media carrying company information. This policy details the handling of media, including storage, transportation, protection and safeguards, and disposal / destruction of media.

- Formal procedures shall be established to ensure safe handling and security of the data that are stored on electronic and print media.

- Access to CD-ROM, floppy, and USB drives shall be granted against authorization from Head – Information Security
- Media (both electronic and print) shall be protected against misuse through password protection and lock and key respectively.
- Media shall be protected from physical damages like fire, moisture and magnetic interference during storage and transportation.
- Formal procedures shall be established all media (including Information Technology (IT) and non IT assets) are appropriately maintained to help ensure its continued availability and integrity.
- A stock or inventory of all the media must be maintained.
- Formal procedures shall be established to review the condition and capacity of IT assets and plan for replacement of IT assets.
- Media shall be disposed off securely and safely when no longer required. The contents of the media shall be made irrecoverable, if the media will be no longer used.
- Formal procedures for the secure disposal of media shall be established to minimize the risk of sensitive and confidential information being disclosed to unauthorized persons.
- Approval for removal of media, destruction / disposal of media shall be sought from appropriate authority and a record of such approvals shall be maintained for audit trail.
- Procedures shall be in place to identify media requiring secure disposal techniques. Approval for the same shall be sought before disposal of media or its contents are carried out.

5. TRAINING

Cloud4C shall ensure all team members undergo periodical training outlined in this policy.

6. REVIEW OF THE POLICY

- Management Review Committee shall review suitability and adequacy Media Handling Policy document during management review meetings
- This document will be reviewed and updated on an annual basis or when significant changes occur to the organization systems and information security standards.

7. COMPLIANCE WITH THE POLICY

Compliance with the Media Handling Policy and Procedure shall be mandatory. Head Information Security–Cloud4C, assisted by information security forum shall ensure continuous compliance to this policy and procedure with in 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.

8. VIOLATION OF THE POLICY

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

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.

9. CONTACT ROLE FOR CLARIFICATION REGARDING THE POLICY

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

10. WAIVER CRITERIA

This Policy and Procedure 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 s 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.