CLOUD4C

2021

MEDIA HANDLING PROCEDURE

Compliance Team

CLOUD4C SERVICES PVT LTD

DOCUMENT CONTROL

Preparation

Draft	Author	Date
1.0	Sudheer G	16/04/2013
1.1	Sudheer G	25/03/2014
1.2	Soudha Rahman	04/03/2015
1.3	Deepthi Naidu	04/02/2016
1.4	M.Venkataniranjan	24/07/2016
1.5	M.Venkataniranjan	13/01/2017
1.6	M.Venkataniranjan	06/01/2018
1.7	Rajendra Kumar	21/05/2018
1.8	M.Venkataniranjan	05/01/2019
1.8	P. Dali Naidu	02/01/2020
1.8	Keerthana Ravikanti	31/12/2020

Classification	Storage Location
Confidential	Shared folder

Review and Approval

Reviewer & Approver	Version	Date	Reviewed Draft Version
RS Prasad Rao	1.0	16/04/2013	1.0
RS Prasad Rao	1.1	25/03/2014	1.1
RS Prasad Rao	1.2	13/04/2015	1.2
RS Prasad Rao	1.3	04/02/2016	1.3
RS Prasad Rao	1.4	25/07/2016	1.4
RS Prasad Rao	1.5	16/01/2017	1.5
RS Prasad Rao	1.6	7/01/2018	1.6
RS Prasad Rao	1.7	22/05/2018	1.7
RS Prasad Rao	1.8	07/01/2019	1.8
RS Prasad Rao	1.8	05/01/2020	1.8
RS Prasad Rao	1.8	01/01/2021	1.8

Release

Release Version	Date Released
1.0	16/04/2013
1.1	25/03/2014
1.2	04/03/2015
1.3	04/02/2016
1.4	24/07/2016
1.5	13/01/2017
1.6	06/01/2018

1.7	22/05/2018
1.8	07/01/2019
1.8	05/01/2020
1.8	01/01/2021

Distribution List

Name	Designation	Department
COE Teams	COE Engineers	Service Delivery
BU Heads		

Change Control

Version	Change Reason	Effective Date
1.0	Baseline	16/04/2013
1.1	Aligned to the Cloud4Cformat, logo, added statement of Confidentiality& Reviewed	25/03/2014
1.2	Reviewed and updated	13/04/2015
1.3	Reviewed and no update	04/02/2016
1.4	Reviewed and Updated version	25/07/2016
1.5	Reviewed and Updated version and scope	16/01/2017
1.6	Reviewed and Updated version control	7/01/2018
1.7	Reviewed and Updated version control	22/05/2018
1.8	Reviewed and Updated version control	07/01/2019
1.8	Reviewed and Updated version control	05/01/2020
1.8	No updates	01/01/2021

STATEMENT OF CONFIDENTIALITY

TABLE OF CONTENTS

1 DESCRIPTION

Cloud4C uses various types of media to store data and information. The main types are paper, compact disks, and magnetic tapes. Media contains confidential client or proprietary information which needs to be appropriately handled.

The following sections describe how to handle different media types and events in the media lifecycle. This document defines the processes and guidelines which shall be followed when handling media, such as tapes, memory sticks, and diskettes, used as part of Cloud4Cinformation system.

2 SCOPE

Cloud4C Services Private Limited 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.

3 REFERENCE POLICY

- Media Handling Policy

4 WORK TASKS

- Media Storage
- Protection Mechanism
- Maintenance of IT Assets
- Review and replacement of IT Assets
- Disposal

5 WORK ACTIVITIES

5.1 Media Storage

All Cloud4C information shall be protected and safeguarded from being leaked out (***Refer**: Information Handling and Labeling Procedure*). Following procedures shall be used to ensure safe handling and security of the data that are stored on electronic and print media.

5.1.1 Electronic Media

Confidential information (***Refer**: Asset Classification and Control Standard*) from the server/ client machine shall be copied to CD/ DVD/ Flash Drives/ external hard drives only with authorization from the respective Departmental Heads. The Departmental Heads shall authorize for media to be moved out of Cloud4C premise and a record of all such movements shall be maintained as audit trails. Before the media is moved out of Cloud4C premise, the data on the media shall be deleted using the procedures mentioned under Data Disposal process (***Refer** Section 3.16 - Data Disposal Procedure in this document*). This would aid in limiting the opportunity for data loss.

5.1.2 Disable Universal Serial Bus (USB) Drives

By default, CD-ROM, floppy, Universal Serial Bus (USB) drives shall be disabled on Cloud4C systems (Desktops, Servers, and Laptops) as applicable. Access to any removable media shall be enabled only if there is a business reason for doing so. Access to CD-ROM, floppy, and USB drives shall be granted against authorization from Head – Information Security. IT administrator shall enable the CD-ROM and floppy drives only on approval from Head - Information Security. All authorized employees shall use only CD'S, floppies and USB device provided by the IT Department. Use of personal CD'S, floppies and USB device is strictly prohibited. Cloud4C has the right to confiscate personal storage device brought into Cloud4C.

5.1.3 Print Media

All printouts and scanned copies of confidential shall be controlled as mentioned in the Information Labeling and Handling Procedure (***Refer**: Information Handling and Labeling Procedure*). The faxes, printers and scanners shall be placed in a secured area. Access to both shall be restricted to ensure that no visitor can gain easy access without notice of the staff. The fax machines and printers shall be protected from heat, pollution and other environmental hazards.

5.2 Protection Mechanism

5.2.1 Password Protection (Electronic Media)

Procedure formulating password protection for softcopy files shall be according to the policies and procedures mentioned in other related policies (***Refer**: ISMS - Access Control Policy and ISMS - Asset Classification and Control Standard*). This shall help secure the files during the creation of the file by password protection.

5.2.2 Lock & Key (Print Media & Other Externally Stored Media)

Procedure formulating secure storage of printed copies under lock and key shall be according to the policies and procedures mentioned in other related policies. (***Refer**: ISMS - Information Labeling and Handling Procedure and ISMS - Asset Classification and Control Standard*). Backup tapes stored at the offsite location shall be stored within fireproof lockers and access shall be restricted to authorized personnel designated by Head – Information Security / Department Heads.

5.2.3 Transportation

In the case of media in transit, reliable transport or couriers shall be used. Packaging shall be adequate to protect the contents from any physical damage likely to arise during transit and under manufacturers' specifications. Special controls shall be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification e. g. Use of locked containers, tamper-evident packaging (which reveals any attempt to gain access). For media leaving the premises, an authorization letter signed by the Head - Information Security/ Departmental Heads shall be sent along with the media. Also, the document shall mention the reason for the media taken out of the premises. This shall be checked by the security guards when the employee takes the media outside the premises of Cloud4C. In the case of transportation of media, Cloud4Cand the Service organization shall identify the person who shall be authorized to transport media in and out of Cloud4C. Only such identified and authorized person shall be allowed to carry out the media outside Cloud4C premises. The

identified person shall sign on the receipt of the media and shall carry the same receipt in the case of media being returned.

5.2.4 Environmental Protection

All media such as hard disks, backup tapes, USB, CD shall be maintained according to the manufacturer's specifications. All these media shall be stored within fireproof lockers and access to the locker shall be restricted to authorized personnel designated by Head – Information Security / Department Heads (***Refer**: ISMS - Physical and Environmental Security Policy*).

5.3 Maintenance of IT Assets

Equipment shall be appropriately maintained to help ensure its continued availability and integrity. Preventive maintenance is an important activity that needs to be carried out on IT hardware to ensure the continuous availability of all the servers and network equipment.

The following controls shall be implemented to achieve that objective:

- Asset Custodians along with the Departmental Heads shall be responsible for ensuring proper maintenance of the Information System Assets within Cloud4C
- Departmental Heads shall maintain a list of all the critical Information System hardware assets along with their maintenance schedules as prescribed by vendors
- Software register that consists of all ICT equipment, workstations. Servers, mobile devices and network devices are maintained so that information sources are monitored and regularly audited on information about new patches or updates
- Typical maintenance activities may consist of the following:
    - Checking hard drive capacity, optimize any local hard drives to defragment files and scan the surface for bad sectors
    - Cleaning up of temp files and backed up log files
    - Regular housekeeping including a dust-free environment, removal of debris from immediate area etc. and the regular checks for integrity of cable installations, including attachment of cable ends, coiling of excess cable lengths, orderly cable runs, and cleanliness of connections
    - Assurance of Uninterruptible Power Supply (UPS), including maintenance of battery installations, cleanliness of power cord junctions and contacts, cleanliness and integrity of grounding straps and conduits, checks of case ground integrity, etc
    - Physical installation integrity, including tightness of rack mounting bolts and screws, slide hardware, and ancillary connections
    - Checking the functioning of backup equipment
- Maintenance activities may vary depending upon the type of hardware and vendor. Asset Custodian with the help of Departmental Heads shall identify maintenance activities required for all IT hardware and prepare a Preventive Maintenance Schedule. It could be a weekly or monthly schedule
- Head - Information Security shall review the maintenance activities carried out by the engineers every quarter
- For all maintenance activities, the Administrators shall ensure that:
    - Preventative maintenance schedule/maintenance activities do not disrupt or impact in any way critical or sensitive applications

  - Maintenance activities are not scheduled during critical periods of data processing or other IT activities such as back up or restoration. All parties shall be notified before any maintenance activity shall be carried
- AMC (Annual Maintenance Contract) and SLA (Service Level Agreements) shall be available for all IT Assets
- If AMC is not required for any IT Assets, necessary approval shall be obtained by Head - Information Security
- Departmental Heads shall maintain stock of all standby equipment and spares in working condition
- Departmental Heads shall also help ensure a standby arrangement for support and equipment with established alternate sources, in the event of failure of support by the regular vendor
- All critical IT assets mainly server and communication equipment will be installed and operated under proper environmental and security conditions
- Equipment shall be maintained under the supplier's recommended service intervals and specifications
- Only authorized maintenance personnel shall be allowed to carry out repairs and service equipment
- Records shall be kept of all suspected or actual faults and all preventive and corrective maintenance
- The maintenance personnel from vendors shall be adequately monitored during maintenance operations carried out in-house
- Applications, operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions
- In case the Information System asset needs to be sent out for maintenance, then documentation shall be prepared to help ensure traceability and accountability. Adequate packing and handling instructions shall be given to the transporter for ensuring physical safety during transit
- Appropriate care shall be taken when sending equipment off-premises for maintenance
- Requirements of insurance policies relating to Information System assets, if any, shall be complied with

5.3.1 Non-IT Equipment (Office Equipment) Management

Fax machines, photocopiers, printers, etc are important equipment for managing day to day operations at Cloud4C. The following procedures shall be followed to ensure that these equipment are working properly and continuously.

- All users of the office equipment shall be adequately trained to ensure that they use them appropriately. They shall operate the equipment as per the guidelines provided by the vendor of the specific equipment
- Ensure that AMC for photocopiers or other equipment are in place
- Operations personnel, at the start of each shift, shall check the fax machines, photocopiers and key printers to ensure that they are working in good condition. If the cartridges are empty, ensure that spare cartridge is in place so that they can be replaced at any point of time that day

- Asset Custodians shall prepare a maintenance schedule considering the AMC available for the equipment. As part of the maintenance schedule, every backup fax machine/printer shall be checked monthly to ensure that they are working in good condition and identified unused printers and MFDs will undergo sanitization process
- Asset Custodians shall perform the Preventive Maintenance as per the schedule and ensure that vendors conduct the preventive maintenance for the equipment as per the AMC
- Head - Information Security shall review the records of maintenance every quarter

5.4 Review & Replacement of IT Assets

- Condition and capacity of existing IT assets should be reviewed periodically. It is recommended that all critical IT equipment are replaced at least once in 5 years to help ensure better availability of the services as most of the equipment would become outdated in 5 years and timely availability of spares and support cannot be help ensured
- Necessary provision shall be made in the annual budget for replacements
- Information stored on media that needs to be available longer than the media lifetime (under manufacturers' specifications) shall be also stored elsewhere to avoid information loss due to media deterioration
- In case of extension of use beyond 5 years, necessary support arrangements shall be signed with the supplier and it shall be approved by Departmental Heads
- Data Center Management Team shall be responsible to monitor end of life with the supplier for all critical IT assets and alert the Departmental Heads for necessary replacements

5.5 Disposal

ICT equipment management policy is being implemented as it is capable of processing, storing or communicating sensitive or classified information on the information it process, stores or communicates is protected appropriately.

Cloud4C has partnered with Avtel Data Destruction company for securely destroying & disposing of the administrator workstations and other ICT equipment. Avtel is an ASIO-T4 certified organization and will be destroying and disposing of the ICT media as per the ASIO-T4 standards. Please refer to the Australian ASIO-T4 guidelines that are followed for media handling & destruction @ https://www.asio.gov.au/asio-t4-protective-security.html.

For server & infrastructure ICT equipment, CDC also has partnered with Avtel Data Destruction Services and ensure the media destruction is also carried out as per ASIO-T4 standards.

6 APPLICABILITY

This procedure document shall apply to all employees of Cloud4C, contractors, subcontractors, and third-party users who have access to Cloud4C information systems and premises.

Exceptions to this policy and procedure may be solely granted by Head – Information Security in consultation and approval from the Information security forum. An employee found to violate

this policy and procedure may face disciplinary action up to and including dismissal from the employment and/or criminal prosecution where the act constitutes a violation of the law.

7 REFERENCE POLICIES, PROCEDURES, & TEMPLATES

- ISMS – Asset Classification and Control Standard
- ISMS – Access Control policy and procedure
- ISMS – Physical and Environmental Security policy and procedure
- ISMS – Information Labeling and Handling procedure
- ISMS – Third Party Management policy and procedure
- ISMS – Media Approval and Gate Pass Template
- ISMS - Preventive Maintenance Schedule Template
- ISMS – Information System Asset / Media Disposal Template
- ISMS – Asset Classification Policy and Procedure

8 ROLE OF EACH ACTIVITY (RACI MATRIX)

	Head - IS	Departmental Head	IT Department	Asset Owners	Administration Department
Media Storage	C, I	C, I,	R, A	C, I	R, I
Protection Mechanism	C,I	C,I	R, A	C,I	R, I
Maintenance of IT Assets	C, I	C, I	R, A	R, I	I
Review and Replacement of IT Assets	R, C	R, C	R, A	C, I	I
Disposal / Destruction	R, C	R,C	R, A	R,C	R, I