02 January 2021

DATA PRIVACY & RETENTION POLICY

Compliance Team

CTRLS DATACENTERS LTD

DOCUMENT CONTROL:

Preparation

Draft	Author	Date
1.0	Venkataniranjan. M	31-01-2017
1.1	Venkataniranjan. M	06-01-2018
1.2	Venkataniranjan. M	10-10-2018
1.2	Venkataniranjan. M	05-01-2019
1.2	P Dali Naidu	02-01-2020
1.2	P Dali Naidu	28-12-2020

Classification	Storage Location
Confidential	Shared Folder

Review & Approval

Reviewer & Approver	Version	Date	Reviewed Draft Version
RS Prasad Rao	1.0	07-02-2017	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	02-01-2021	1.2

Release

Release Version	Date Released
1.0	07-02-2017
1.1	07-01-2018
1.2	10-10-2018
1.2	07-01-2019
1.2	03-01-2020
1.2	02-01-2021

Distribution List

Name	Designation	Department

COE Engineers	COE Teams	Service delivery
All BUs	BU Heads & Employees	

Change Control

Version	Change Reason	Effective Date
1.1	Reviewed with no updates	07-01-2018
1.2	Reviewed and added 6.3 V)VM Deletion in private cloud VI)Storage Deletion in private cloud Training section - 7 Review of the policy section -8	10-10-2018
1.2	No updates	05-01-2019
1.2	Reviewed and no updates	03-01-2020
1.2	Reviewed and no updates	02-01-2021

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 OVERVIEW

This policy covers the privacy practices that CtrlS and its associates follow when providing Managed services, Cloud or another services to its customers. CtrlS establishes this privacy policy in order to clarify on the use of data which it may be in its possession due to the nature of certain services it provides.

2 OBJECTIVE:

CtrlS is committed to protect information and data of Client. This Privacy Policy deals with the security and privacy requirements for maintaining, disclosing and disposing of customer identifiable information.

3 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 facility

4 REFERENCE DOCUMENTS

- ISO/IEC 27001 standard, clauses A.5.1.1, A.7.1.2, A.12.4.1, A.12.4.2, A.14.3.1, A.16.1.2 and A.18.1.4
- ISO/IEC 27017 standard, clauses 5.1.1, 12.4.1 and 16.1.2
- ISO/IEC 27018 standard, clauses 5.1.1, 11.2.7, 12.4.1, 12.4.2, 12.4.3, 16.1.2, A.1.1, A.2.1, A.2.2, A.5.1, A.5.2, A.7.1, A.9.1, A.9.2, A.10.1 and A.10.2
- Information Security Policy
- Statement of Applicability
- Acceptable Usage Policy
- Media Handling Policy
- Network Security Policy
- Access Control Policy
- Risk Management Policy
- Business Continuity Policy
- Cloud data security policy
- Data classification policy
- Data Protection Policy
- Document and Data Control Process
- Private Cloud Data Protection Policy
- Customer Account Life Cycle
- Insider Threat Policy
- Encryption Policy
- List of Legal, Regulatory and Contractual and Other Obligations
- Incident Management Procedure
- Media Handling Procedure

5 BASIC PII TERMINOLOGY

PII principal – the person to whom the PII refers.

Personally Identifiable Information (PII) – any information that, by means of use or correlation with other data or information, can be used to uniquely identify an entity. Group of PII referred as Configuration items.

"Customer Configuration" means an information technology system (hardware, software and/or other information technology components) which is the subject of the Services or to which the Services relate.

"**Customer Data"** means all data which Customer receives, stores, or transmits on or using the Customer Configuration.

Derivative Data means data or information, created, generated from use of customer data or configuration.

Direct Data classifies items such as name, address, birthplace, marital status and occupation.

Cloud service provider – party which makes cloud services available according to the cloud model.

Processing of PII Operation or set of operations performed on personally identifiable information (PII).

Sub-processor" means any Data Processor (including any third party) appointed by the Processor to process Controller Personal Data on behalf of the Controller.

6 PII

Personally Identifiable Information (PII) – any information that, by means of use or correlation with other data or information, can be used to uniquely identify an entity.

- **First or last name (if common)**
- **Date of birth**
- **Country, state or city of residence**
- **Telephone numbers**
- **Email addresses**

Public PII (Non-sensitive) is easily accessible from public sources like phonebooks, the Internet, and corporate directories.

Public PII include (Non-sensitive):

- Visiting Cards
- Business telephone number
- Business mailing or email address
- Employment information
- Zipcode
- Gender
- Financial information

1. The above list contains pieces of information and examples of non-sensitive information that can be released to the public. This type of information cannot be used alone to determine an individual's identity.
2. However, non-sensitive information, although not delicate, is linkable. This means that non-sensitive data, when used with other personal linkable information, can reveal the identity of an individual.

CtrlS Role as Cloud PII processor

3. Based on the service specifications given by the customer, CtrlS performs customer configuration of IT Infrastructure building, allocation of capacity, IP segmentation, VPN control, patch, PPM activities, back-up activities and delivers to the customer. However CtrlS role is limited to management of customer infra.

4. As a cloud service provider CtrlS cloud may have PII/customer data related to Cloud customer which is purely owned/visible and accessible by customer only. All the access rights to the customer sensitive data (PII) remains with customer. CtrlS doesn't have ownership/accessibility to the data. CtrlS is only hosting services.

6.1. THE DATA WE COLLECT ABOUT YOU

Cloud4C will not collect any personally identifiable information about individual unless it is provided to us voluntarily.

Generally, we collect personal information (P-PII) related to customers, employees, and representatives when they decide to interact with us, or avail services or get status updates and communication about services. We also look at how they interact with us so that we can offer the best possible experience.

We have grouped together as follows:

- Identity Data: including first name, last name.
- Contact Data: including billing address, Business telephone number, Business mailing or email address

For which purposes and on which legal basis do we use your personal data?

- Cloud4C uses personal information (P-PII) only where required for specific purposes..

Purpose	Legal basis
Perform any legally required reporting and respond to legal process.	Compliance with a legal obligation.
Customers billing address, email address, and telephone numbers and prospective clients information	• Where we need to perform the contract, we are about to enter into or have entered into with customers. • Where it is in our legitimate interests, including our commercial

	interests in operating the Cloud4C customer facing platforms.

- Where the above table states that we rely on our legitimate interests for a given purpose, we are of the opinion that our legitimate interests are not overridden by your interests, rights or freedoms, given (i) the transparency we provide on the processing activity.

6.2. HOW WE PROTECT YOUR PERSONAL DATA?

We are committed to protecting Public personal Information. We put in place safeguards including appropriate technologies, policies, and contractual arrangements, so that the data we have about customers is protected from unauthorized access and improper use.

The safeguards we have put in place to protect your personal data include:

- Technical and Organizational Measures

7 POLICY

CtrlS is committed to provide complete control to the customer over the use, and distribution of their data.

Under extant law and as per contractual terms, data of any Customer hosted on CtrlS network will be treated as “Customer Data”. CtrlS treats any information confidential to Customer, confidential and takes all reasonable measures to safeguard the confidentiality of the Customer Data. Customer owns complete ownership of the data. CtrlS have no control whatsoever over the content of the information passing through its network and/or on the Customer's website(s).

8 DATA LOCATION

- CtrlS provides an option for customers to choose and know exact geographic locations where their data resides unless prohibited by applicable law in force.
- The CtrlS informs to the cloud service customer on the geographical locations of the cloud service provider can store the cloud service Customer Data (PII).
- CtrlS maintains transparency on Customer Data (PII) by providing information on where the Customer Data (PII) will reside on the cloud. To that end, and to serve its Customers better, CtrlS maintains an ever-expanding network of Data centres around the globe and verifies that each data centres meets stringent security requirements.

- CtrlS uses your Customer Data (PII) only to the extent such data is required to provide the services agreed upon, and does not mine it for marketing or advertising. In case a Customer decides to suspend the services or terminates the requirement for availing services, CtrlS shall, in accordance with Customer's requirements, and any applicable laws, and other policies it has, follows strict standards and requisite processes for deleting Customer Data (PII) from its servers.

8.1 INFORMATION STORAGE

To ensure the protection of PII submitted to CtrlS, all assets used to store PII must make use of best practices. In situations where such practices are unavailable, the use of practices must be authorized by SD Head and documented.

8.2 TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define the current security measures established by Cloud4C. These may change at any time without notice by keeping a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without diminishing the security level.

a. External Audits will be conducted annually once. Any gaps identified in the audit, will be addressed with corrective action for information security and the public cloud operations.
b. Maintain Information security policies and make sure that policies and measures are regularly reviewed and where necessary, improve them
c. Communication with Cloud4C applications utilizes cryptographic protocols such as TLS to protect information in transit over public networks.
d. Data security controls which include logical segregation of data, restricted (e.g. role-based) access is used.
e. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions.
f. Password controls designed to manage and control password strength, and usage including prohibiting users from sharing passwords.

g. Change management procedures and tracking mechanisms to designed to approve and monitor all changes to Cloud4C technology and information assets.
h. Incident / problem management procedures design to allow Cloud4C investigate, respond to, mitigate and notify of events related to Cloud4C technology and information assets.
i. Vulnerability assessment, patch management, and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.
j. **Physical Access Control:**

Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms where data processing systems are located.

Measures:

All **Data Centers** adhere to strict security procedures enforced by guards, surveillance cameras, access control mechanisms and other measures to prevent equipment and **Data Center** facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the **Data Center** facilities. To ensure proper functionality, physical security equipment (e.g. cameras, etc.) are maintained on a regular basis. In detail, the following physical security measures are implemented at all **Data Centres**:

   i. Cloud4C protects its assets and facilities using the appropriate means based on a security classification conducted by security department.
   ii. In general, buildings are secured through access control systems (smart card access system).

8.3 ACCESS CONTROLS

- CtrlS has put in place strong measures to protect data from inappropriate/un-authorized access, including limits on CtrlS personnel and subcontractors from accessing Customer Data (PII). However, nothing contained herein prevents Customer from accessing its own data at any time and for any reason unless prohibited by any law or judicial or executive order in force.
- In accordance with Customer's requirements, CtrlS creates access controls at the time of initial setup, then handovers the same to the customer. Customer may, in its

absolute discretion change the access controls and CtrlS has no access to the Customer's data irrespective of nature of services unless specifically required by Customer under any written contract.

8.4 INFORMATION USE AND SHARING

CtrlS ensures that Personally Identifiable Information processed, will be used only for the following purposes:

- Purposes defined in the contract with the cloud service customer
- Technical support required to fulfill the customer's contract
- Granting user access

8.5 DATA TRANSFERS

- CtrlS has developed and designed data security practices to ensure that Customer Data (PII) is appropriately protected. Customer Data (PII) may be transferred as per contractual obligations so long as they are not repugnant to any applicable Law in force. CtrlS complies with all applicable relevant laws in force on Data Privacy regarding the collection, use, and retention of Customer Data (PII).
- CtrlS recommends that all the communication between Customer's users and Customer's platforms be done over https to ensure protection of users' sensitive data.

8.6 TO PROVIDE SERVICES AND TO FIX ISSUES.

- CtrlS provides legal and compliance teams with a comprehensive repository of information resources designed to help them understand and verify the compliance requirements of the customer's cloud deployments. To Provide Services and to Fix Issues.
- CtrlS will provide services as per agreed terms under contract to provide Cloud or other services. This may include applying new product or system versions, patches, updates and upgrades; monitoring and system use and performance; and other issues reported to CtrlS.
- Based on the request raised by the customer, CtrlS accesses customer setup to resolve particular issue. CtrlS will use temporary access to fix the issue raised by the Customer within agreed time window.

8.6.1 IN RESPONSE TO THE LAW.

CtrlS may disclose Customer’s information if it required to comply with a law, regulation, or valid legal process. If CtrlS is going to disclose Customer’s information, CtrlS will provide Customer with a notice unless it is prohibited from doing so under law or under judicial or executive order. Further, CtrlS may disclose Customer’s information without providing customer with a prior notice if it reasonably be required that such disclosure is necessary to prevent imminent and serious harm to a person.

9 CONTENT

- All hosting services provided by Cloud4C may be used for lawful purposes only. Transmission, storage, or presentation of any information, data or material in violation of any Indian law is prohibited. This includes, but is not limited to copyrighted material, trade secret, material in our opinion is obscene, not in public interest, opposed to public policy or is an invasion of privacy of any person or entity.
- The Customer agrees to indemnify and hold harmless Cloud4C from any claims resulting from the use of the service which damages the Customer or any other party.
- Any attempt to undermine or cause harm to any of the servers of Cloud4C is strictly prohibited. Cloud4C shall take no responsibility for the use of its clients' accounts by the Customer.
- In case of abuse of the resources provided by Cloud4C, in any way, Cloud4C reserves the unqualified right to immediately deactivate the Customer’s account, without refund.
- It shall be responsible for any misuse of its account and it must take steps to ensure that others do not gain unauthorized access to its account. It shall not use its account to breach the security of another account or attempt to gain un-authorised access to another network or server.

10 INFORMATION SECURITY ROLES AND RESPONSIBILITIES

By ensuring that roles and responsibilities are clearly defined we will be in a good position to prevent many data protection incidents affecting personal data from happening and to react effectively and appropriately if and when they do.

10.1 DATA PROTECTION OFFICER

CtrlS will assign a point of contact (Data Protection Officer) for processing PII and has specific responsibilities for the protection of the personal Information. The DPO (Data Protection

Officer) is responsible to coordinate all activities necessary to ensure the proper application of this policy.

The Data Protection Officer has the following responsibilities:

- Monitor compliance with the policies in relation to the protection of personal information
- Provide advice where requested regarding data protection impact assessments and monitor their performance
- Cooperate with all relevant supervisory authorities for data protection
- Act as the contact point for supervisory authorities on issues relating to personal data processing and to consult, where appropriate, with regard to any other matter.

10.2 DEPARTMENT MANAGERS

Department Managers may be heads or supervisors of operational units within the organisation.

A Department Manager has the following responsibilities:

- Review and manage employee competencies and training needs to enable them to perform their role effectively within the data protection area
- Ensure that employees are aware of the relevance and importance of their activities and how they contribute to the achievement of data protection objectives
- Participate in, and contribute to, data protection assessments affecting their business area

10.3 EMPLOYEES

The responsibilities of all employees are defined in a variety of organisation-wide policies and are only summarized in brief below.

An employee has the following main responsibilities:

- Ensure they are aware of and comply with all data protection policies of the organisation relevant to their business role
- Report any actual or potential security breaches
- Contribute to data protection assessment where required.

11 TRAINING

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

12 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.

13 COMPLIANCE WITH THE POLICY

CtrlS privacy Policy shall be mandatory. Head Information Security– CtrlS, assisted by information security forum shall ensure continuous compliance with this policy and procedure with in CtrlS. Periodic review is to be conducted by Departmental Heads and the same to be reported to Head – Information Security to verify compliance with this policy and procedure. All employees are required to inform the Head– Information Security, if any policy breach is discovered or identified.

13.1 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 as determined by an investigation.

14 CONTACT ROLE FOR CLARIFICATION REGARDING THE POLICY

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

15 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 and the non-compliance with the policy will be limited to a specific period of time (subject to a maximum period of 30 days). On 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.