03 January 2020

ORGANISATION PRIVACY & RETENTION POLICY

Compliance Team

CLOUD4C SERVICES PVT LTD

DOCUMENT CONTROL:

Preparation

Draft	Author	Date
1.0	M.Venkataniranjan	30-03-2017
1.1	M.Venkataniranjan	06-01-2018
1.2	M.Venkataniranjan	10-10-2018
1.2	M.Venkataniranjan	05-01-2019
1.2	M.Venkataniranjan	02-01-2020
1.2	M.Venkataniranjan	29-12-2020

1.1 REVIEW & APPROVAL

Reviewer and Approver	Version	Date	Reviewed Draft Version
R.S.Prasad Rao	1.0	16-04-2017	1.0
R.S.Prasad Rao	1.1	07-01-2018	1.1
R.S.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

1.2 RELEASE

Release Version	Date Released
1.0	16-04-2017
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

1.3 DISTRIBUTION LIST

Name	Designation	Department
NOC Teams	SM Managers	
COE Teams	COE Leads	

1.4 CHANGE CONTROL

Version	Change Reason	Effective Date
1.1	Reviewed with no updates	07-01-2018
1.2	Reviewed and added Training section - 7, Review of the policy section - 8	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	02-01-2021

STATEMENT OF CONFIDENTIALITY

This document contains proprietary trade secret and confidential information to be used solely for evaluating Cloud4C 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 Cloud4C Datacenters Ltd.

CONTENTS

2 OVERVIEW

In its everyday business operations Cloud4C collects and stores records of many types and in a variety of different formats. The relative importance and sensitivity of these records also varies and is subject to the organisation's security classification scheme.

It is important that these records are protected from loss, destruction, falsification, unauthorised access and necessary controls are used to ensure this, including backups, and access control.

Cloud4C 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.

3 OBJECTIVE:

Cloud4C is committed to protect information and data. This Privacy Policy deals with the security and privacy requirements for maintaining, disclosing and disposing of identifiable information.

4 SCOPE

This policy 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 facility

5 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

6 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.

7 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

6.1. SENSITIVE PERSONAL IDENTIFYING INFORMATION (PII)

Sensitive Personal Identifying Information (PII) is defined as information that if lost, compromised, or disclosed could result in substantial harm, inconvenience, or unfairness to an individual.

Sensitive PII include:

- Bank account numbers
- Passport information
- Driver’s license

6.2. HIGHLY SENSITIVE PII INCLUDE:

- Healthcare related information
- Medical insurance information
- Biometric data: Finger print or voice signatures

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

6.1. NON-SENSITIVE OR PUBLIC PII INCLUDE:

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

- 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.
- 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.

8 POLICY

- Cloud4C is committed to process PII in accordance with its responsibilities stated in the privacy Policy.
- PII is collected for specified, explicit and legitimate purposes only
- PII processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised processing and against destruction or damage, using appropriate technical or organisational measures.

- Personal data is stored for longer periods insofar as the personal information will be processed solely for archiving purposes in the Business interest
- Cloud4C also has a responsibility to ensure that it complies with all relevant legal, regulatory requirements in the collection, storage, retrieval and destruction of records.

9 DATA PRIVACY PRINCIPLES

8.1. THE DATA WE COLLECT ABOUT YOU

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

We may collect, use, store and transfer different kinds of personal data which we have grouped together as follows:

- Identity Data: including first name, last name.
- Contact Data: including billing address, email address, and telephone numbers.

8.2. HOW IS YOUR PERSONAL DATA COLLECTED?

Generally, we collect personal information related to customers, employees, and representatives when they decide to interact with us, or avail services or express an interest or apply for a position. We also look at how they interact with us so that we can offer the best possible experience.

8.3. HOW WE USE YOUR PERSONAL DATA

We may use personal information for the following purposes:

- to provide services to the relevant member or groups of members
- to engage in activity in relation to our member services. This may include sending updates, meeting invite and other information that may be of important.
- where anyone has applied for a position with us, to review and process job application
- to comply with legal or regulatory obligations that we must discharge
- To verify identify and entitlements to our products and services when you contact us or access our services.
- To supply services and manage payments.
- To send statements and invoices, and collect payments.
- To provide commercial quotes.
- To provide technical and customer support.
- To obtain feedback on our services.
- To provide improved website and product experience and communications informed by product subscriptions and/or data collected.

We will only use personal data when the law allows us to. Most commonly, we will use personal data in the following circumstances:

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

- Cloud4C uses personal information only where required for specific purposes..

Purpose	Legal basis
Managing our contractual and/or employment relationship with you.	Necessary for the performance of a contract to which you are a party.
Recruitment.	Justified on the basis of our legitimate interests for ensuring that we recruit the appropriate employees.
Facilitating communication with you (including in case of emergencies, and to provide you with requested information).	Justified on the basis of our legitimate interests for ensuring proper communication and emergency handling within the organization.
Operating and managing our business operations.	Justified on the basis of our legitimate interests for ensuring the proper functioning of our business operations.
Complying with legal requirements.	Necessary for the compliance with a legal obligation to which we are subject.
Monitoring your use of our systems (including monitoring the use of our website and any apps and tools you use).	Justified on the basis of our legitimate interests of avoiding non-compliance and protecting our reputation.
Improving the security and functioning of our website, networks and information.	Justified on the basis of our legitimate interests for ensuring that you receive an excellent user experience and our networks and information are secure.
Marketing our products and services to you (Refer Cloud4C.com/privacy-policy).	Justified on the basis of our legitimate interests for ensuring that we can conduct and increase our business.
Specific Recruitment/Employment Purposes	Legal basis
Assess your suitability for employment for the role for which you are applying, as well as future roles that may become available.	Justified on the basis of Cloud4C's legitimate interests of ensuring that it recruits the appropriate employees.
Manage your application.	Justified on the basis of Cloud4C's legitimate interests of ensuring that it recruits the appropriate employees.
Perform data analytics, including analysis of our applicant pool in order to better understand who is applying to positions and how to attract and keep top talent.	Justified on the basis of Cloud4C's legitimate interests of ensuring that it continually improves its recruitment processes.
In some cases, record your online interview for review by additional recruiters and hiring managers.	Justified on the basis of Cloud4C's legitimate interests of ensuring that it recruits the appropriate employees.
If you register for any position.	Justified on the basis of Cloud4C's legitimate interests of ensuring that it recruits the appropriate employees.

Transfer your contact information, education data, employment data, application information and the CV, all as supplied by you in our recruitment system, to the Cloud4C Talent acquisition Team.	Justified on the basis of Cloud4C's legitimate interests of ensuring that it recruits the appropriate employees.
Administration of employee benefits	Justified on the basis of Cloud4C's legitimate interests of ensuring that our employees receive the applicable benefits.
Perform any legally required reporting and respond to legal process.	Compliance with a legal obligation.
To share alumni information with other internal Cloud4C systems, specifically our internal sales tool (salesforce.com), to contact you with industry relevant information.	Justified on the basis of our legitimate interest for ensuring proper communication with, and sending marketing to, our alumni.
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.

8.4. DATA MINIMISATION

- Cloud4C shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

8.5. HOW WE SHARE YOUR PERSONAL DATA

We may share personal data with one or all of the following:

- Internal Third Parties: these include other companies within the Cloud4C Services Pvt Ltd. such as Cloud4C, TIER4..etc

External Third Parties may include:

- Suppliers who we engage to provide services on our behalf, for example payment processors and marketing services companies
- Authorities who require reporting of processing activities in certain circumstances.

8.5.1. VENDOR HAVING ACCESS TO PII?

Service or work involving vendor access to PII include:

- A contractor is hired to provide payroll service to assist organisation Performance Management system. The potential exists for the contractor to have access to PII of employee such as names, mailing addresses, salary slip, personal telephone numbers, and financial account information.
- A vendor or contractor is hired to perform survey on the organisation work culture or corporate program to be used by Organisation Top Management. Depending on the nature of the survey, the vendor or contractor may have access to PII such as names of the survey respondents, email addresses, ..etc.
- A contractor is hired to deploy or upgrade physical access control systems (e.g., card swipe entry readers) and Biometric access card. The potential exists for the contractor to have access to any PII collected via the card swipe and thumb impression such as names, Organisation ID numbers and finger print.

8.6. HOW WE PROTECT YOUR PERSONAL DATA?

We are committed to protecting personal data. 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

8.6.1. ACCURACY

- Cloud4C shall take reasonable steps to ensure personal data is accurate

8.7. KEEPING YOUR INFORMATION AND INFORMATION SECURITY

How long we hold personal information for will vary and will depend principally on:

- the purpose for which we are using personal information - we will need to keep the information for as long as is necessary for the relevant purpose, and
- Legal obligations - laws or regulation may set a minimum period for which we have to keep personal information.
- We will ensure that the personal information that we hold is subject to appropriate security measures.
- Access to personal information is limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- When personal data is deleted this should be done safely such that the data is irrecoverable.
- Appropriate back-up and disaster recovery solutions shall be in place.

8.8. ARCHIVING / REMOVAL

- To ensure that personal data is kept for no longer than necessary, the Cloud4C implements retention period for each area in which personal data is processed and review this process annually.

- The retention period shall consider what data should/must be retained, for how long, and why.

8.9. YOUR CHOICES AND RIGHTS

These rights include:

- Obtaining information regarding the processing of personal information and access to the personal information which we hold.
- Please note that there may be circumstances in which we are entitled to refuse requests for access to copies of personal information. In particular, information that is subject to legal professional privilege will not be disclosed other than to our member and as authorised by our member.
- Requesting that we correct personal information if it is inaccurate or incomplete.
- Requesting that we erase personal information in certain circumstances. Please note that there may be circumstances where we erase personal information but we are legally entitled to retain it.
- Objecting to, and requesting that we restrict, our processing of personal information in certain circumstances. Again, there may be circumstances where you object to, or ask us to restrict, our processing of personal information but we are legally entitled to refuse that request.
- Withdrawing your consent, although in certain circumstances it may be lawful for us to continue processing without your consent if we have another legitimate reason (other than consent) for doing so.

9. DATA LOCATION

9.1. INFORMATION STORAGE

To ensure the protection of PII submitted to Cloud4C, 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.

9.2. PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION IN CLOUD ENVIRONMENTS

The DPO (Data Protection Officer) is responsible to coordinate all activities necessary to ensure the proper application of this policy.

9.3. RECORD TYPES AND GUIDELINES

- In order to assist with the definition of guidelines for record retention and protection, records held by Cloud4C are grouped into the categories listed in the table on the last page. For each of these categories, the required or recommended retention period and allowable storage media are also given, together with a reason for the recommendation or requirement.

- Note that these are guidelines only and there may be specific circumstances where records need to be kept for a longer or shorter period of time. This should be decided on a case by case basis as part of the design of the information security elements of new or significantly changed processes and services.

9.4. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, , unauthorised disclosure of, or access to, personal data, the Cloud4Cl promptly assess the risk to people's rights and freedoms and if appropriate report the Top Management and Cert-in.

9.5. RECORD RETRIEVAL

There is little point in retaining records if they are not able to be accessed in line with business or legal requirements. The choice and maintenance of record storage facilities must ensure that records can be retrieved in a usable format within an acceptable period of time. An appropriate balance should be struck between the cost of storage and the speed of retrieval so that the most likely circumstances are adequately catered for.

9.6. RECORD DESTRUCTION

Once records have reached the end of their life according to the defined policy, they must be securely destroyed in a manner that ensures that they can no longer be used. The destruction procedure must allow for the correct recording of the details of disposal which should be retained as evidence.

9.7. RECORD REVIEW

The retention and storage of records must be subject to a regular review process carried out under the guidance of management to ensure that:

- The policy on records retention and protection remains valid
- Records are being retained according to the policy
- Records are being securely disposed of when no longer required
- Legal, regulatory and contractual requirements are being fulfilled
- Processes for record retrieval are meeting business requirements.

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

Cloud4C will assign a point of contact (Data Protection Officer) for processing PII and has specific responsibilities for the protection of the personal Information.

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. DOCUMENT MANAGEMENT

Cloud4C creates and maintains the following security and privacy documentation as well as store them in a central repository with restricted access control:

a. DPA and DPA Exhibit
b. Technical and Organizational Measures
c. Non-disclosure Agreement (NDA) or similar(as required)
d. Sub-processor Agreement (as required)

11.1. SECURITY MEASURES

This document describes technical and organizational security measures and controls implemented by Cloud4C to protect personal Information and ensure the ongoing confidentiality, integrity and availability of Cloud4C's products and services.

This document is a high-level overview of Cloud4C's technical and organizational security measures. Cloud4C reserves the right to revise these technical and organizational measures at any time, without notice, so long as any such revisions will not materially reduce or weaken the protection provided for personal Information that Cloud4C processes.

a. Organizational management is responsible for the development, implementation, and maintenance of Cloud4C's Privacy program.
b. Maintain Information security policies and make sure that policies and measures are regularly reviewed and where necessary, improve them.

11.2. 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.

11.2.1. PHYSICAL ACCESS CONTROL:

Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms where data processing systems are located which process and/or use **Personal Information**.

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).
iii. Depending on the security classification, buildings, individual areas and surrounding premises are further protected by additional measures. These include specific access profiles, video surveillance and biometric access control systems.
iv. Access rights will be granted to authorized persons on an individual basis according to the System and Access Control measures (see Section 2.2 and 2.3 below). This also applies to visitor access. Guests and visitors to buildings must register their names at reception and must be accompanied by authorized personnel. Cloud4C and all third party **Data Center** providers are logging the names and times of persons entering the private areas within the **Data Centers**.

11.2.2. SYSTEM ACCESS CONTROL:

Data processing systems used to store data must be prevented from being used without authorization.

Measures:

i. Authorization level is used to grant access to sensitive systems including those storing and processing **Personal Data**. Processes are in place to ensure that authorized users have the appropriate authorization to add, delete, or modify users.

ii. Cloud4C has procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If a user leaves the company, its access rights are revoked.

iii. Cloud4C has established a password policy that prohibits the sharing of passwords, governs what to do if a password is disclosed, requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form.. Each computer has a password-protected screensaver.

iv. The company network is protected from the public network by firewalls.

v. Cloud4C uses up–to-date antivirus software on all workstations.

vi. A security patch management is implemented to ensure deployment of relevant security updates.

11.2.3. . DATA ACCESS CONTROL:

Persons entitled to use data processing systems shall gain access only to the **Personal Information** that they have a right to access, and **Personal Information** must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

Measures:

i. Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. All personal, confidential, or otherwise sensitive Information is protected in accordance with the security policies and standards.

ii. All production servers of any Service are operated in the relevant **Data Centers**/server rooms. Security measures that protect processing personal, confidential or other sensitive information are regularly checked. To this end, Cloud4C conducts internal and external security checks and penetration tests on the IT systems.

iii. Cloud4C does not allow the installation of personal software or other software not approved by management to their systems being used for any Cloud Service.

iv. Cloud4C security standard governs how Information and Information carriers are deleted or destroyed.

11.2.4. DATA TRANSMISSION CONTROL:

Personal Information must not be read, copied, modified or removed without authorization during transfer.

Measures:

i. **Personal Information** transfer over Cloud4C internal networks are protected as any other confidential data according to Cloud4C's Security Policy.

11.2.5. DATA INPUT CONTROL:

It shall be possible to retrospectively examine and establish whether and by whom at Cloud4C **Personal Information** have been entered, modified or removed from data processing systems.

Measures:

i. Cloud4C only allows authorized persons to access **Personal Information** as required in the course of their work.

11.2.6. JOB CONTROL:

Personal Data being processed on commission shall be processed solely in accordance with the Agreement and related instructions of Privacy Policy.

Measures:

i. As part of the Cloud4C Security Policy, Personnel Information requires at least the same protection level as “confidential” information according to the Cloud4C Information Classification standard.
ii. All Cloud4C employees and contractual partners are contractually bound to respect the confidentiality of all sensitive information of customers and partners.

11.2.7. AVAILABILITY CONTROL:

Personal Information shall be protected against accidental or unauthorized destruction.

Measures:

i. Cloud4C uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability to the **Data Centers**.
ii. Emergency processes and systems are regularly tested.

11.2.8. DATA INTEGRITY CONTROL

Ensures that **Personal Information** will remain intact, complete and current during processing activities:

Measures:

i. This refers to controls as stated in the control and measure sections as described above. In particular:
    - Firewalls;
    - Security Monitoring Center;
    - Antivirus software;
ii. Change management procedures and tracking mechanisms to designed to approve and monitor all changes to Cloud4C technology and information assets.
iii. Incident / problem management procedures design to allow Cloud4C investigate, respond to, mitigate and notify of events related to Cloud4C technology and information assets.
iv. Security Incidents

Cloud4C maintains an incident response plan and follow documented incident response policies including data breach notification where a breach is known or reasonably suspected.

12. TRAINING

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

13. 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.

14. COMPLIANCE WITH THE POLICY

Cloud4C privacy Policy shall be mandatory. Head Information Security– Cloud4C, assisted by information security forum shall ensure continuous compliance with this policy and procedure with in Cloud4C. 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.

14.1. 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.

15. CONTACT ROLE FOR CLARIFICATION REGARDING THE POLICY

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

16. 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.

17. APPENDIX A

No	Department	Data/Record	Data Mode	Disposal Policy/period	Accountable Head/Role
