Table of Contents

Document Control

Role	Tittle
Document Name	**Data Privacy Policy**
Document Number	**CMSRS/ISMS/Data/R0**
Auditor	
Contributors	
Quality Controls	

Release Version

Version	Release date	Released by
1.0	**04-Dec-2020**	**IT Head**

Release Version

Version	Release date	Change Log	Process and Recommended Head-IT Approved	Approved By CE
1.0	**04-Dec-2020**	**Initial Document release**	**Jobin T.Akkara**	**Subba Rao**

1.0 Introduction

Chola MS Risk Services (referred as CMSRS) shall protect and safe-keep any customer information including personal identified information wherever it has interconnection provided to it in recognition of its responsibility to use such information in an appropriate and responsible manner. CMSRS shall implement technology and security features and strict policy guidelines to safeguard the privacy of the customer information from unauthorized access or improper use. CMSRS shall implement a process to identify frauds and assess the likelihood and impact of various types Risk of frauds through periodic monitoring and reporting to the top management in order to prevent any irregularities to the information assets of CMSRS.

2.0 Reference Policy

- ISMS - Information Security Policy.

3.0 Work Tasks

The key tasks identified in this procedure are:

- Customer Privacy
- Personal Identifiable Information Protection
- Customer Information Protection

3.1 Work Activities

3.1.1 Customer Privacy

3.1.1.1 Customer Choice

CMSRS shall respect customer (or web-site visitor) choices in respect of privacy of customer information. A customer or visitor may choose not to receive direct marketing communications from CMSRS in connection with their services. Upon such choice, CMSRS (a) shall not contact that customer or web site visitor directly with marketing messages about their services, and (b) shall not use customer or web site visitor identifiable information obtained from that customer or web site visitor's registration for or use of an online service to contact that customer or web site visitor with marketing messages about any CMSRS' products or services.

3.1.1.2 Protection of customer or web-site visitor identifiable information

Customer-identifiable information which a visitor volunteers at one of CMSRS web sites to order CMSRS products shall be protected just as if the information had been provided under more traditional ways of ordering that service.

CMSRS shall implement technology and security features and strict policy guidelines to safeguard the privacy of the customer identifiable information from unauthorized access or improper use, and shall continue to enhance security procedures as new technology becomes available.

3.1.1.3 Usage of customer identifiable information

CMSRS shall also use customer identifiable information to investigate and help prevent potentially unlawful activity or activity that threatens the network or otherwise violates the customer agreement for that service.

3.1.1.4 Correction of account information

CMSRS honour's requests from customers to review all customer identifiable information maintained in reasonably retrievable form, which currently consists of the customer name, address, e-mail address, telephone number and/or billing information, and shall correct any such information which may be inaccurate. Customers may verify that appropriate corrections have been made.

3.1.2 Personally Identifiable information and protection

Information which can be used to distinguish or trace an individual's identity, such as his/her name, social security number, biometric records, etc called PII. Any information which, if lost, compromised or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. It includes any one or more of the types of information that are outlined below:
Date and time when you accessed our website;
Your IP address;
Name and version of your browser;
The website (URL) which you visited before accessing our website, and
Certain cookies
As part of the conclusion of a contract or the initiation of such, we will also gather the following information:
first and last name, e-mail address and other information which you provide;
There is no obligation for you to actually provide the data which we request from you. However, if you do not, you will not be able to use all of the functions of the website, and we will usually not conclude the contract or carry out the order, or will no longer be able to carry out an existing contract and will have to terminate it.

- Maintaining Personal Identifiable Information (PII)

During the course of normal job responsibilities, CMSRS may come in contact with PII, either already existing in CMSRS network, or as part of a business process. Because PII requires special handling due to potential risk associated with its disclosure, it is important to 1) verify the need for the existence of PII in the CMSRS network and 2) ensure that the information is properly secured.

- Verify the need to collect PII

CMSRS shall collect the least amount of information in order to follow standard business procedures. Caution should especially be taken when collecting PII. The need to collect the information should be periodically reviewed.

- Collection Procedures

If PII does need to be collected, CMSRS shall make sure that the data is secured. Any PII data collected should not be stored on the local workstation; it would need to reside in secured server with required encryption/masking.

- Verifying the need to store PII

Whenever PII is found residing in the CMSRS network, a determination needs to be made regarding whether the information is needed for an existing business practice, or if it can be securely disposed. If the information does need to be retained, contact IT department for guidance on the best means to secure or dispose of the information properly.

- Authorized dissemination of PII

In the event an outside entity would need to have any data that includes PII, said entity would need to confirm that they understand the sensitivity of the information, and the need to properly safeguard it. Transport of data should be done through secure means (ideally shared through encryption or secured transport are necessary.

- Unauthorized dissemination of PII

In the event of an unauthorized disclosure or access of PII:

- Report the incident to your Functional Head & CISO
- Send an email to ciso@cholams.murugappa.com
  - Do NOT forward any compromised information in the email
  - Include the location of the information (email or network location)
  - If email, include the sender and subject (unless the subject contains the PII)
  - Include any other relevant details, such as location and contact phone number
- Comply with the instructions from the Incident Response Team

3.1.3 Customer information protection

- Customer information shall be acquired for specific intended purposes and to the extent necessary for the achievement thereof.
- Intended purposes shall be made readily known to the customers concerned at any time.
- Legal and proper means shall be used for acquiring customer information. Special attention shall be paid if any customer information is to be acquired from a third party. Specifically, it shall be confirmed that the third party used legal and proper means to acquire the relevant information. In addition, care shall be exercised to avoid unduly harming the interests of the customers concerned (including their privacy).
- Customer information may be used only to the extent necessary for the achievement of its intended purposes.

- Customer information shall not be provided to any third parties (excluding our partners) except in the following cases:
- where the prior consent of each relevant customer has been obtained;
- where the extent of the provision of the customer information to a subcontractor or any other party is limited to the achievement of the intended purposes concerned;
- where the use of the customer information is shared between or among specific parties, and the intended purposes, the parties to which such information is to be provided, and other details have already been notified to each customer concerned or publicized; or
- where any legal provision requires the customer information to be provided, or the customer information otherwise needs to be provided for the public good.
- If an agent requests that customer information be provided, all of the following documents shall be obtained, and the details thereof shall be checked before the actual provision of said information.
- a letter of proxy (bearing the principal's registered seal)
- the principal's seal-registration certificate (one issued within three [3] months)
- a document proving the status of the agent

The accuracy of customer information shall be kept as high as possible in accordance with the following rules:

- Customer information shall be kept accurate and up-to-date to the extent necessary for the achievement of the intended purposes.
- Customer information shall be disposed of or otherwise processed as soon as it becomes unnecessary for business use.
- Reasonable security measures shall be taken to prevent (i) leakage, loss, obliteration, and damage and (ii) unauthorized access, use, destruction, tampering, and the like.

If the handling of customer information is to be contracted out to a third party, a trustworthy subcontractor shall be selected, and measures shall be taken, for example, by including certain provisions in the subcontracting agreement. Such provisions shall
(i) Restrict the use of the information to be provided, thereby making the information usable only within the scope of the subcontracted operations, (ii) ensure confidentiality, and (iii) assign liability for damages. (Refer ISMS: Third Party Management policy and procedure)

If a customer makes a request involving any disclosure, revision, or the like of information regarding the customer himself or herself, and if the request is deemed to be legitimate, then the request shall be accommodated within a reasonable period upon positive identification of the customer.

Customer information shall be properly stored, accessed, disposed of, and so forth in accordance with the Asset Classification Standard (Refer ISMS: Asset Classification and Control Standard and Information Labeling and Handling Procedure).

3.1.3.1 Protection of on-line transactions

CMSRS shall collect and use customer identifiable information for billing purposes, to provide and change service, to anticipate and resolve problems with the service, or to create and inform customers of products and services that better meet customer needs. This means that CMSRS may use customer identifiable information, in conjunction with information

available from other sources, to market new services to customers that CMSRS think will be of interest to them. However, CMSRS shall take consent from customers before sharing information.

Description

CMSRS may collect ‘usage data’ when customers, or any other third parties, visit CMSRS websites. This "usage data" may include a record of which pages a Web browser has visited. CMSRS may use usage data to provide advertising about products and services that may be of interest to customers, or to provide customized features and services.

Description

CMSRS and advertising agencies contracted by CMSRS may use various kinds of software devices to collect information about Internet use. Small files called "cookies" may be attached to customer or (Web page) visitor Web browser. These files identify individual browsers and save information such as passwords so that Web sites can recognize the customer or (Web page) visitor. In addition, on some Web sites,
CMSRS and advertising agencies contracted by CMSRS may use small bits of code called "single-pixel gifs," or "clear gifs" embedded in some Web pages, to make cookies more effective.

CMSRS may use contracted advertising companies to deliver ads. The advertising companies may also receive some anonymous information about ad viewing by Internet users on CMSRS Web sites and other Internet sites. This information may be associated with a customer's or visitor’s Web browser, but shall not be associated with a name or e-mail address without the customer's or visitor’s explicit permission.

3.1.3.2 Disclosure

CMSRS shall not sell, trade, or disclose to third parties any customer identifiable information derived from the registration for or use of CMSRS service - including customer names and addresses - without the consent of the customer (except as required by legal processes or in the case of imminent physical harm to the customer or others).

When CMSRS uses other agents like IT service provider, contractors or group/partner companies to perform services on its behalf, CMSRS shall help ensure that the company protects customer identifiable information consistent with this Policy.

E-mail Contents: The company shall not read or disclose to third parties private e-mail communications that are transmitted using CMSRS’ services except as required to operate the service or as otherwise authorized by law.

4.0 Changes to This Policy

We are committed to upholding the principles of privacy and data protection. We therefore examine our data protection policy at regular intervals in order to ensure that it is free of errors and is situated in a highly visible place on our website. We also ensure that it contains appropriate information about your rights and our processing work, and that it has been created according to the relevant legislation and therefore complies with it. We may update this data protection policy occasionally in order to keep it up to date, in order to take new developments into account, and to ensure adherence to the applicable

legislation. If we were to make considerable changes to this data protection policy, we would inform you of this by giving notice of it on our website and via an updated version of the data protection policy.

5.0 Constraints

Nil

6.0 Date of Rollout

This policy shall come into force along with other IS Policies as presented and approved by the MISF.