## PURPOSE

To plan for the Information Security management system to address the internal and external issues of OEC and the requirements of the interested parties as defined in Chapter 3.

## SCOPE

Applicable to the Information Security management system at the Head office and warehouse located at Dheku.
Pickup, Storage (Physical and Media), Retrieval and Forwarding, Permanent Returning or Pre Destruction Services for Customer Records at Dekhu location and supporting activities from Head Office at Vashi.

## REFERENCE

NA

## RESPONSIBILITY

The overall responsibility for meeting the above objectives lies with the Chief Operating Officer.

## DESCRIPTION OF ACTIVITIES

1. Actions to address risk and opportunities:

1.1 General:

1.1.1 Information Security Management System planning is carried out considering :

1.1.1.1 Internal and External Issues

1.1.1.2 Needs and Expectations of Interested Parties

1.1.1.3 Risk and Opportunities:

1.1.2 Information Security Management System ensures :

1.1.2.1 Information Security management system shall achieve its purpose.

1.1.2.2 Prevent or reduce undesired effects of Information Security breach.

1.1.2.3 Achieve continually improvement

1.1.3 Risk and Opportunities are reviewed, analyzed and acted upon to ensure Information Security Management System meets the expectations.

1.1.4 Actions are integrated and implemented into Information Security Management System processes and effectiveness of these actions are evaluated.

1.2 Information Security Risk Assessment:

1.2.1 information security risk assessment process is established and maintained to ensure

1.2.1.1 Norms' for Information Security Risk, Risk acceptance and Risk assessment performance are established.

1.2.1.2 Consistency exists for repeated Information Security risk assessment and provide valid and comparable results.

1.2.1.3 Information Security risks and its owners are identified for loss of confidentiality, integrity and availability of information as per scope of Information Management System.

1.2.1.4 Information Security risks are analyzed to assess to determine potential consequences, its probability of occurrence to determine level of risk.

1.2.1.5 Information Security risks are evaluated against risk criteria to prioritise risk treatment plan.

1.2.2 Records of Information Risk Assessment is maintained.

1.3 Information Security Risk Treatment:

1.3.1 Based on Risk Assessment results appropriate Information Security Risk Treatment options are selected and controls are determined.

1.3.2 Adequacy of controls are verified with requirement of ISO 28001:2013 Annexure A to workout Statement of Applicability. Justification for Exclusion if any is also addressed.

1.3.3 Information Security Risk Treatment Plan is developed; Residual Information Security risks are determined and approved by Risk owner.

1.3.4 Information Security Risk Assessment and Risk Treatment is carried out as per Process of Information Security Risk Management

1.3.5 Records of Information Risk Treatment is maintained

2.0 Information Security objectives and planning to achieve them:

2.1.1 Information Security Objectives are established at relevant functions and levels ensuring:

2.1.1.1 Information Security Objectives are Consistent with the Information Security policy and considering Risk assessment and Risk Treatment requirement.

2.1.1.2 Target for Information Security objectives are Measurable

2.1.1.3 Performance of Information Security objective is periodically monitored

2.1.1.4 Objectives are communicated to concerned persons.

2.1.1.5 Objectives are updated as per requirements

2.2 Planning actions to achieve Information Security objectives:

2.2.1 Information Security objectives are communicated to concerned person of organization.

2.2.2 Action plan to achieve Information Security Objective are defined elaborating what to do, who shall do, target date, resource need and how to evaluate results. If require target is broken into smaller mile stones to monitor progress.

2.2.3 Information Security Objectives and its action plan are documented in Information Security Objective

## ENCLOSURES

NA

## FORMATS / EXHIBITS

NA