

DEPARTMENT		ISSUE DATE	REVISION #
MR	OEC-MR-QS-M-01	2016-09-14	0.0
	CHAPTER 2 – INFORMATION SECURITY MANAGEMENT SYSTEM POLICY AND OBJECTIVES		PAGES 1 of 1

Policy and Objectives

The objective of information security policy is to maintain and improve information security to ensure the business continuity of the Organisation. This is also to minimize the risk of damage by preventing security incidents and reducing their impact for the services rendered in the space of records management.

The policy's goal is to protect the organization's informational assets against all internal, external, deliberate or accidental threats.

The information policy has been approved by the VP - IT and the security policy ensures that:

1. The confidentiality of corporate and customer information is assured.
2. Sensitive information (however stored) will be protected against unauthorised access.
3. The integrity of information is maintained.
4. Information will be made available to business processes and authorized employees only as and when required.
5. Regulatory and legislative requirements are met;
6. Business continuity plans for mission critical activities are in place, maintained and tested.
7. Information security awareness training is given to all the employees including permanent and contract employees if any.
8. All breaches of information security, actual or suspected are reported to the information Security Manager and thoroughly investigated.
9. Business requirements for availability of information and systems are met.
10. The Information Security Policy (ISP) exists and OEC complies with ISO 27001 standards.
11. The Information Security Manager is responsible for the maintenance of this policy and to provide support and advice during its implementation.
12. All functional managers are directly responsible for ensuring policy compliance by their staff in their respective departments.
13. Compliance with the Information Security Policy is mandatory.